Consiglio Nazionale delle Ricerche
Istituto di Calcolo e Reti ad Alte Prestazioni

# Vulnerability Assessment su server di progetto ICAR-CNR

Antonio Francesco Gentile, Rosa Varchera, Andrea Vinci

**RT-ICAR-CS-24-02** **Maggio 2024**

Consiglio Nazionale delle Ricerche, Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR)
– Sede di Cosenza, Via P. Bucci 8-9C, 87036 Rende, Italy, URL: www.icar.cnr.it
– Sezione di Napoli, Via P. Castellino 111, 80131 Napoli, URL: www.icar.cnr.it
– Sezione di Palermo, Via Ugo La Malfa, 153, 90146 Palermo, URL: www.icar.cnr.it

# Sommario

# Abstract

Il presente documento ha lo scopo di evidenziare e riportare i risultati della Analisi delle Vulnerabilità di alcune macchine di progetto interne all'ICAR-CNR, e di discutere il risultato delle azioni correttive intraprese per risolvere le vulnerabilità identificate e per mitigare i rischi relativi alla sicurezza delle stesse.

# Introduzione

Secondo la definizione dell'Istituto Nazionale gli Standard e la Tecnologia statunitense (NIST), una vulnerabilità è una debolezza in un sistema informativo[1]. Una valutazione delle vulnerabilità fornisce a un'organizzazione non solo informazioni sulle falle di sicurezza presenti nei suoi sistemi, ma anche indicazioni su come valutare i rischi associati alle vulnerabilità individuate. La cybersecurity è diventata una priorità per le aziende di ogni settore, considerando la crescente minaccia di violazioni della sicurezza informatica. Il 75% di tutte le violazioni della rete sono causate da falle di sicurezza in un'applicazione Web e un dato allarmante è che il 63% delle app Web non viene mai nemmeno testato. L'analisi delle vulnerabilità, essendo un'attività non intrusiva, dovrebbe avvenire ogni 3 o 6 mesi, così da prevenire al meglio minacce emergenti e garantire alle organizzazioni elevati standard di sicurezza.

Nel seguente lavoro vengono descritti i concetti di vulnerability e di vulnerability assessment, evidenziando alcuni dei possibili attacchi che un sistema informatico potrebbe subire. Viene descritto il processo di identificazione e valutazione dei punti deboli della sicurezza nei sistemi informatici, nelle reti e nelle applicazioni e alcuni dei tool più importanti utilizzati per la ricerca di vulnerabilità. Seguendo le metodologie descritte sono stati effettuati test di analisi su tre host diversi, nella fase pre vengono riscontrate delle vulnerabilità sugli host che poi sono state sanificate come è chiaramente mostrato nelle tabelle, nei grafici e nei relativi report post sanificazione. Ad oggi non risultano data breach, i dati presenti sulle macchine non risultano essere stati compromessi o esposti a persone o organizzazioni non autorizzate. Le conseguenze di un data breach possono essere gravi ecco perché vulnerability assessment periodici diventano fondamentali.

[1] National Institute of Standards and Technologies (NIST) U.S.A. - Guide for Conducting Risk Assessments – Settembre 2024. Url: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

# Vulnerability

Nel contesto della sicurezza informatica, una vulnerabilità è un difetto, una debolezza o una lacuna in un dispositivo, un processo, un database, un software, un'infrastruttura, un sistema o una rete (o un insieme di controlli specifici) che i criminali informatici possono sfruttare. Le vulnerabilità comuni possono essere affrontate rapidamente tramite patch o aggiornamenti, ma le vulnerabilità appena scoperte richiedono tattiche di rimedio approfondite. Se non vengono corrette, le vulnerabilità possono essere sfruttate per ottenere un accesso non autorizzato e danneggiare la rete aziendale. In generale, esistono due tipi di vulnerabilità:

1. Vulnerabilità tecniche: Si tratta di carenze nel software o nell'hardware, come codice difettoso o bug delle applicazioni.
2. Vulnerabilità umane: Queste sono legate all'elemento umano presente in qualsiasi sistema o rete bersaglio. I dipendenti possono essere vittime di e-mail di phishing, smishing o altri vettori di attacco comuni. Possono anche condividere accidentalmente le credenziali del proprio account o lasciare un endpoint non protetto.

La necessità del Vulnerability Assessment è generalmente sottovalutata, è noto solo per essere una pratica formale e per essere utilizzato da pochissimi individui. Utilizzando un Vulnerability Assessment frequente ed efficace, è possibile ridurre significativamente l’esposizione agli attacchi e fornire applicazioni più sicure.

# Vulnerability Assessment

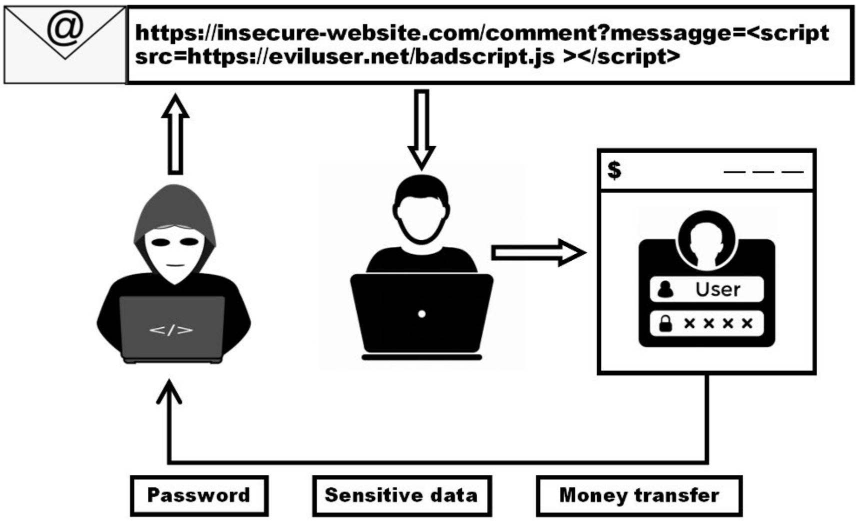
Vulnerability assessment, conosciuto anche come analisi delle vulnerabilità, è un processo che definisce, identifica e classifica le falle di sicurezza (vulnerabilità) di un'infrastruttura di comunicazione che può interessare la rete o le singole macchine. La vulnerabilità nella sicurezza di rete è definita come un difetto o una debolezza nella rete o nel sistema, che un qualsiasi attaccante può sfruttare. Più il sistema di rete è vulnerabile, maggiore è la possibilità che venga attaccato. Uno degli aspetti chiave di questa tipologia di analisi è l’isolamento tempestivo delle vulnerabilità evidenziate che potrebbero causare un blocco temporale o una grave perdita di dati. Avere un buon strumento di vulnerability assessment permette di avere una visione aggiornata del livello di sicurezza, indispensabile per stabilire se si è a rischio di un attacco informatico. Il più grande vantaggio di una vulnerability assessment è che può prevedere il successo delle contromisure proposte ed esaminare l'effettivo tasso di successo dopo la loro applicazione. Questo processo viene tipicamente intrapreso per analizzare in modo proattivo l'infrastruttura di sicurezza di un’organizzazione, identificare le potenziali vulnerabilità derivanti da configurazioni di sistema errate, abuso di computer da parte dei dipendenti o carenze di software e hardware.

Di seguito vengono riportate alcune delle vulnerabilità che possono essere prevenute attraverso il vulnerabilty assessment:

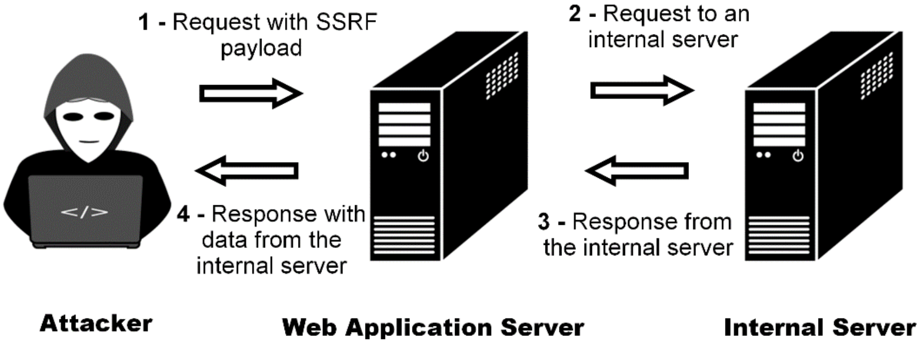
1. **Cross-site scripting (XSS):** è una vulnerabilità della sicurezza web che consente a un aggressore di compromettere le interazioni degli utenti con un'applicazione vulnerabile. Gli attacchi XSS sono rivolti al codice (detto anche script) di una pagina web in esecuzione nel browser dell'utente, senza attaccare direttamente il server del sito web. Le vulnerabilità di cross-site scripting normalmente permettono a un aggressore di mascherarsi come un utente vittima, di eseguire qualsiasi azione che quell'utente è in grado di eseguire e di accedere a qualsiasi dato dell'utente. Esistono tre diversi tipi di XSS attack:

- Reflected XSS
- Stored XSS
- DOM-based XSS

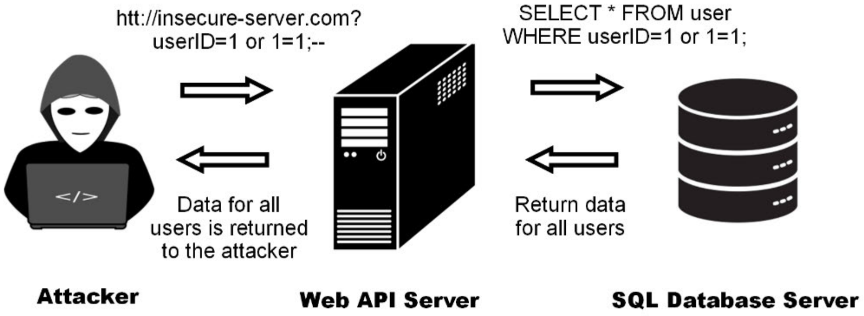
Il Reflected XSS è la varietà più semplice di cross-site scripting. Si verifica quando un'applicazione riceve dati in una richiesta HTTP e li include nella risposta immediata in modo non sicuro. Lo Stored XSS (noto anche come XSS persistente o di secondo ordine) si verifica quando un'applicazione riceve dati da una fonte non attendibile e li include nelle sue risposte HTTP successive in modo non sicuro. Il DOM-based XSS si verifica quando un'applicazione contiene JavaScript lato client che elabora dati da una fonte non attendibile in modo non sicuro, di solito scrivendo i dati nel DOM.


https://insecure-website.com/comment?messagge=<script src=https://eviluser.net/badscript.js ></script>
</>
$
User
××××
Password
Sensitive data
Money transfer

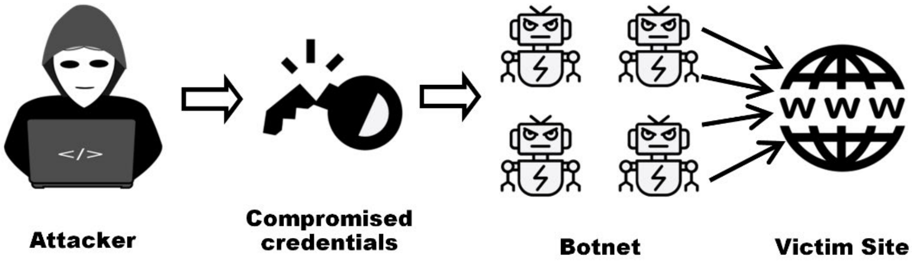
2. **Server-side request forgery (SSRF):** è una vulnerabilità della sicurezza web che consente a un utente malintenzionato di far sì che l'applicazione lato server effettui richieste a una posizione non prevista. Un attaccante potrebbe essere in grado di forzare il server a connettersi a sistemi esterni arbitrari e questo potrebbe far trapelare dati sensibili, come le credenziali di autorizzazione.


1 - Request with SSRF payload
2 - Request to an internal server
</>
4 - Response with data from the internal server
3 - Response from the internal server
Attacker
Web Application Server
Internal Server

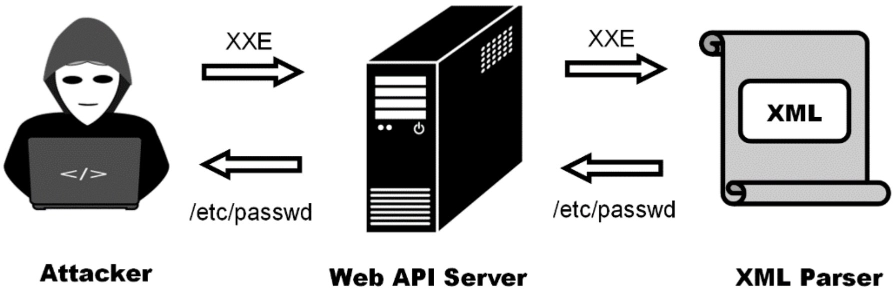
3. **SQL injection**: è una vulnerabilità che consente a un utente malintenzionato di interferire con le query che un'applicazione effettua sul proprio database. Ciò può consentire a un utente malintenzionato di visualizzare dati che normalmente non è in grado di recuperare. Questi potrebbero includere dati che appartengono ad altri utenti o qualsiasi altro dato a cui l'applicazione può accedere. In molti casi, un utente malintenzionato può modificare o eliminare questi dati, causando modifiche persistenti al contenuto o al comportamento dell'applicazione. Un attacco SQL injection riuscito può portare all'accesso non autorizzato a dati sensibili, quali:
    - Password
    - Dati relativi alla carta di credito
    - Informazioni personali degli utenti



4. **Broken Authentication**: è una vulnerabilità di sicurezza che si verifica quando i meccanismi di autenticazione e gestione delle sessioni di un'applicazione web sono difettosi o implementati in modo improprio. L'autenticazione si riferisce al processo di verifica dell'identità degli utenti, in genere attraverso nomi utente e password, mentre la gestione della sessione comporta il mantenimento e il controllo della sessione dell'utente dopo l'autenticazione



5. **XML External Entities (XXE):** è una vulnerabilità della sicurezza web che consente a un utente malintenzionato di interferire con l'elaborazione dei dati XML da parte di un'applicazione. Spesso consente a un utente malintenzionato di visualizzare i file sul filesystem del server dell'applicazione e di interagire con qualsiasi sistema back-end o esterno a cui l'applicazione stessa può accedere. In alcune situazioni, un aggressore può intensificare un attacco XXE per compromettere il server sottostante o un'altra infrastruttura back-end, sfruttando la vulnerabilità XXE per eseguire attacchi SSRF (server-side request forgery).



La valutazione delle vulnerabilità gioca un ruolo fondamentale in ogni tipo di applicazione informatica, sistemi e infrastrutture. Esistono diversi tipi di valutazione della vulnerabilità, questi includono:

1. **Host assessment.** La valutazione delle vulnerabilità basata sull'host funziona su un modello client-server in cui il client esegue la scansione e invia il rapporto al server/gestore. Gli strumenti di valutazione della vulnerabilità basati sull'host possono fornire una visione dei danni potenziali che

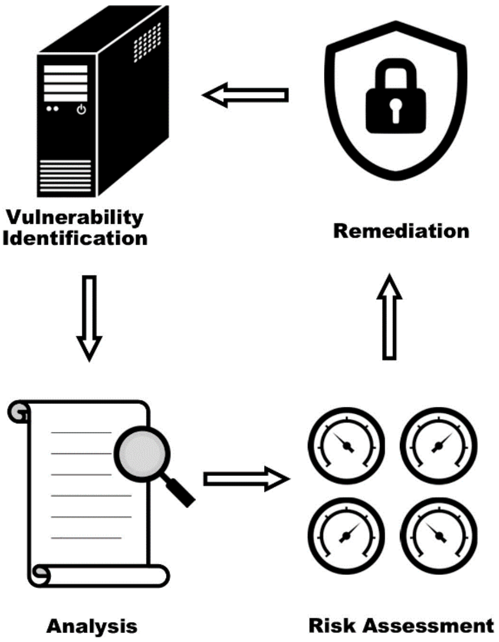
possono essere causati da insider e outsider una volta concesso o ottenuto un certo livello di accesso a un sistema. Gli scanner basati sull'host rilevano i segni che un intruso si è già infiltrato in un sistema. Queste tracce di hackeraggio includono nomi di file sospetti, nuovi file inaspettati, file di dispositivo trovati in luoghi inaspettati e SUID/SGID che hanno potenzialmente ottenuto i privilegi di "root".

2. **Network assessment.** Questi tipi di strumenti consentono di identificare ed eliminare le vulnerabilità di sicurezza delle reti locali. L'analisi basata sulla rete verifica e tiene sotto controllo l'intera rete e non solo uno specifico host. Uno strumento di valutazione della rete affidabile può aiutare a identificare eventuali problemi nella rete. Inoltre, fornisce informazioni sulle aree menzionate di seguito:
   - Utilizzazione delle risorse. Uno strumento di valutazione della rete affidabile aiuta a identificare le risorse sottoutilizzate o sovrautilizzate nella rete e ad allocare tali risorse in modo più efficiente.
   - Colli di bottiglia. Attività come lo streaming di video, l'esecuzione di programmi ad alta intensità di banda o il download di file e programmi di grandi dimensioni possono rallentare notevolmente la velocità della rete. Uno strumento di valutazione della rete aiuterà a identificare e a correggere i famosi colli di bottiglia nella propria rete.
   - Falle di sicurezza. Aiuterà anche a individuare le falle di sicurezza che richiedono un'attenzione immediata.

3. **Database assessment.** È un gruppo di test che possono essere eseguiti su un database. Tale criterio è specifico per un tipo di database (Oracle, MySQL, ecc.) e per una versione o un gruppo di versioni. Questa valutazione suggerisce le priorità di interveno necessarie e possibili miglioramenti futuri. Esamina elementi quali l'entità dei dati duplicati, l'adozione da parte degli utenti e l'esperienza del personale, l'integrazione con strumenti e applicazioni di terze parti e l'utilizzo di oggetti e campi.

# Security scanning process

Il processo di scansione della sicurezza si compone di quattro fasi: Vulnerability Identification, Analysis, Risk Assessment e Remediation.



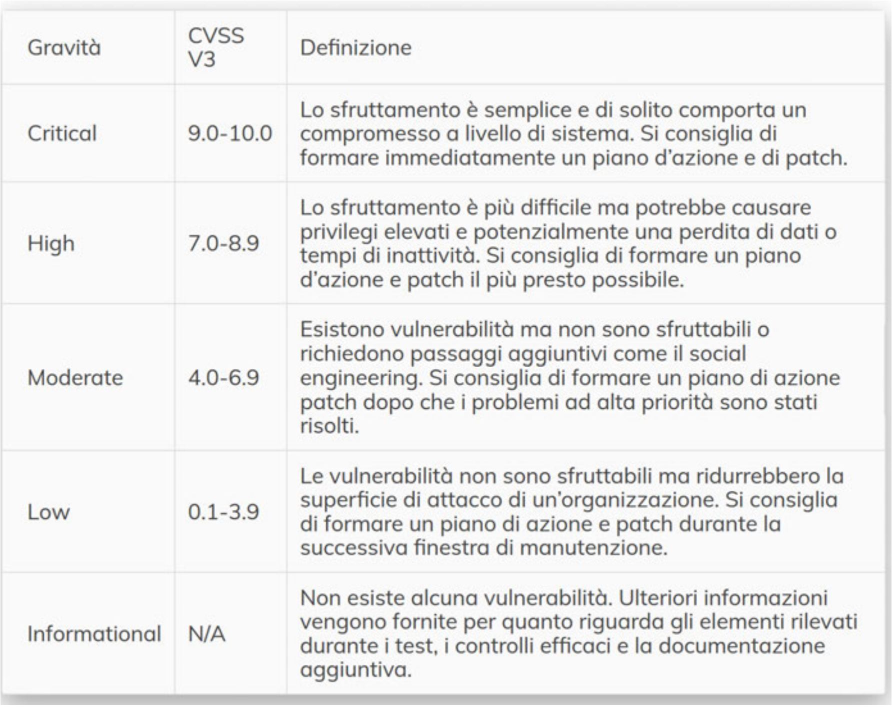
1. **Vulnerability Identification**: è parte integrante delle valutazioni di vulnerabilità, che aiutano a comprendere i rischi per i sistemi, le risorse, i dati e le persone, sia che si tratti di credenziali compromesse o di applicazioni non patchate. L'implementazione di una valutazione basata su framework consolidati come il Cyber Security Framework del NIST o i Critical Security Controls del CIS(Center for Internet Security) fornisce una tabella di marcia completa per un programma di sicurezza informatica solido e basato sul rischio. L'obiettivo di questa fase è redigere un elenco completo delle vulnerabilità di un'applicazione. Viene verificato lo stato di sicurezza eseguendo scansioni con strumenti automatici o testandoli e valutandoli manualmente. I benefici del Vulnerability Identification sono:
    - Enhanced Visibility: Migliorare la visibilità della superficie di attacco è la chiave per una efficace mitigazione del rischio, è necessario conoscere quanto un sistema sia esposto e le vulnerabilità specifiche prima di poter agire con correttivi.
    - Prioritized Risks: Non tutte le minacce informatiche hanno lo stesso impatto, l'identificazione delle vulnerabilità consente di concentrarsi su quelle che creano i rischi maggiori.
    - Actionable Data: Conoscere esattamente le azioni correttive da intraprendere le soluzioni tecnologiche di sicurezza più adatte al caso d'uso
    - Consistent Coverage: Scoprire le vulnerabilità in tutto l'ambiente è un modo di non lasciare lacune nelle difese e di mitigare i rischi in modo coerente.
    - Improved Posture: Identificando le vulnerabilità, è possibile creare una roadmap che dia priorità alle azioni da intraprendere nei prossimi 3, 6 e 12 mesi, migliorando costantemente la posizione di sicurezza.
2. **Vulnerability Analysis**: L'obiettivo di questa fase è identificare l'origine e la causa principale delle vulnerabilità identificate nella fase uno. L'analisi delle vulnerabilità è forse la fase più importante del processo di valutazione delle vulnerabilità, in quanto consiste nell'analizzare se una vulnerabilità segnalata rappresenta effettivamente una minaccia per i propri sistemi . La capacità di identificare

accuratamente le vulnerabilità in questa fase avrà un impatto diretto sulla linea d'azione necessaria da intraprendere.

3. **Risk assessment**: è il processo di identificazione, analisi e valutazione del rischio. Aiuta a garantire che i controlli di sicurezza informatica scelti siano adeguati ai rischi che l'organizzazione deve affrontare. Identifica le risorse che potrebbero essere colpite da un attacco informatico (come hardware, sistemi, laptop, dati dei clienti e proprietà intellettuale) e i rischi che potrebbero colpire tali risorse.
4. **Remediation**: L'obiettivo di questa fase è la chiusura delle lacune di sicurezza, determinando il percorso più efficace per la correzione o la mitigazione di ciascuna vulnerabilità. Questa è una delle fasi più importanti del processo di gestione delle vulnerabilità, fondamentale per proteggere le reti, prevenire la perdita di dati e garantire la continuità aziendale. La correzione delle vulnerabilità comporta la correzione e la neutralizzazione dei potenziali problemi di sicurezza attraverso il processo di valutazione del rischio dell'organizzazione. Questa procedura può ridurre significativamente la possibilità di perdita di dati, violazioni di dati, attacchi DDoS, malware e phishing. Il primo passo della bonifica delle vulnerabilità consiste nel correggere le vulnerabilità relative a codice inadeguato e a configurazione errata del software. Infatti, le vulnerabilità software più comuni includono processi di autenticazione o controlli di sicurezza mal implementati.

# Common vulnerability scoring system

Il Common Vulnerability Scoring System (CVSS) è uno standard industriale libero e aperto per la valutazione della gravità delle vulnerabilità della sicurezza dei sistemi informatici[2]. Il CVSS cerca di assegnare punteggi di gravità alle vulnerabilità, consentendo a chi risponde di dare priorità alle risposte e alle risorse in base alla minaccia. I punteggi sono calcolati in base a una formula che dipende da diverse metriche che approssimano la facilità e l'impatto di un exploit. I punteggi variano da 0 a 10, con 10 che rappresenta la massima gravità. Sebbene molti utilizzino solo il punteggio CVSS Base per determinare la gravità, esistono anche punteggi temporali e ambientali, che tengono conto rispettivamente della disponibilità di mitigazioni e della diffusione dei sistemi vulnerabili all'interno di un'organizzazione. CVSS è composto da quattro gruppi di metriche: Base, Minaccia, Ambientale e Supplementare. Il punteggio di base riflette la gravità di una vulnerabilità in base alle sue caratteristiche intrinseche, che sono costanti nel tempo, e presuppone l'impatto ragionevole del caso peggiore in diversi ambienti di distribuzione. Le metriche di minaccia modificano la gravità di una vulnerabilità in base a fattori quali la disponibilità di codice proof-of-concept o lo sfruttamento attivo. Le metriche ambientali affinano ulteriormente il punteggio di gravità risultante per uno specifico ambiente informatico. Esse considerano fattori quali la presenza di mitigazioni in quell'ambiente e gli attributi di criticità del sistema vulnerabile. Infine, le Metriche supplementari descrivono e misurano ulteriori attributi estrinseci di una vulnerabilità, con lo scopo di aggiungere contesto. Di seguito viene riportata la tabella che mostra i punteggi assegnati ad ogni tipo di gravità.



| Gravità | CVSS V3 | Definizione |
|---|---|---|
| Critical | 9.0-10.0 | Lo sfruttamento è semplice e di solito comporta un compromesso a livello di sistema. Si consiglia di formare immediatamente un piano d'azione e di patch. |
| High | 7.0-8.9 | Lo sfruttamento è più difficile ma potrebbe causare privilegi elevati e potenzialmente una perdita di dati o tempi di inattività. Si consiglia di formare un piano d'azione e patch il più presto possibile. |
| Moderate | 4.0-6.9 | Esistono vulnerabilità ma non sono sfruttabili o richiedono passaggi aggiuntivi come il social engineering. Si consiglia di formare un piano di azione patch dopo che i problemi ad alta priorità sono stati risolti. |
| Low | 0.1-3.9 | Le vulnerabilità non sono sfruttabili ma ridurrebbero la superficie di attacco di un'organizzazione. Si consiglia di formare un piano di azione e patch durante la successiva finestra di manutenzione. |
| Informational | N/A | Non esiste alcuna vulnerabilità. Ulteriori informazioni vengono fornite per quanto riguarda gli elementi rilevati durante i test, i controlli efficaci e la documentazione aggiuntiva. |

[2] Forum of Incident Response and Security Teams. “Common Vulnerability Scoring System Version 3.0 Calculator”. Visitato il 29 Aprile 2024. Url: https://www.first.org/cvss/calculator/3.0

# Vulnerability assessment tools

I Web Application Vulnerability Scanner sono strumenti automatizzati che analizzano le applicazioni web, normalmente dall'esterno, alla ricerca di vulnerabilità di sicurezza come XSS, SQL Injection, Command Injection, Path Traversal e configurazione insicura del server. Questa categoria di strumenti viene spesso definita strumento per il test dinamico della sicurezza delle applicazioni (DAST). Sono disponibili numerosi strumenti di questo tipo, sia commerciali che open source, che presentano tutti punti di forza e di debolezza, i più famosi sono:

- **Acunetix**: è uno scanner di vulnerabilità web che dispone di una tecnologia di crawling avanzata per trovare vulnerabilità in ogni tipo di pagina web, anche quelle protette da password. È in grado di rilevare le vulnerabilità di sicurezza molto rapidamente. Il tasso di errore è davvero basso. Inoltre, rende il lavoro molto più semplice grazie alle sue capacità di integrazione. Acunetix crea automaticamente un elenco di tutti i siti web, applicazioni e API e lo mantiene aggiornato. Non viene lasciato nessun potenziale punto di accesso non scansionato e vulnerabile agli attacchi. Acunetix automatizza la valutazione e la gestione delle vulnerabilità web utilizzando uno dei motori più veloci e accurati del mercato. Individua tutte le vulnerabilità comuni, le configurazioni errate e le debolezze trascurate e verifica quali vulnerabilità sono reali e non falsi positivi. Acunetix si integra con il sistema da analizzare, in modo che le vulnerabilità non arrivino mai in produzione e vengano eliminate rapidamente e senza sforzo.

- **BeSECURE**: è uno scanner di vulnerabilità self-service di Beyond Security che può essere implementato in sede, nel cloud o in ambienti ibridi. Questa soluzione offre una scansione sia della rete che delle applicazioni web e dispone di un database delle vulnerabilità aggiornato quotidianamente. BeSECURE si concentra su efficienza e precisione. La configurazione è semplice e gli utenti possono iniziare in pochi minuti grazie a un'interfaccia pratica e alle funzionalità di automazione. Le sue capacità di test sono le più accurate e la sua reportistica fornisce esattamente le informazioni necessarie per riparare le vulnerabilità che possono causare la perdita di dati. Riesce a mappare e a valutare la rete per mostrare in tempo reale quali sono i componenti di rete più vulnerabili agli attacchi e dove indirizzare gli interventi di bonifica. Scansiona automaticamente tutto ciò che "parla IP": server, infrastrutture, workstation, endpoint di qualsiasi tipo, stampanti, IoT inclusi. Ogni scansione include la più ampia gamma di test di sicurezza oggi disponibile e la libreria dei test di beSECURE viene ampliata per includere spesso nuove vulnerabilità, con aggiornamenti ogni ora. beSECURE testa il comportamento degli host di rete registrando le loro risposte offrendo un'accuratezza simile a quella dei test di penetrazione.

- **Burp Suite**: è uno scanner di vulnerabilità web che viene aggiornato frequentemente e si integra con sistemi di tracciamento dei bug come Jira per la semplice generazione di ticket. Lo scanner di vulnerabilità web che sta alla base della popolarità di Burp Suite ha qualcosa in più rispetto agli altri. Burp Scanner utilizza la ricerca leader mondiale di PortSwigger per aiutare i suoi utenti a trovare automaticamente un'ampia gamma di vulnerabilità nelle applicazioni web. Burp Scanner è il cuore di

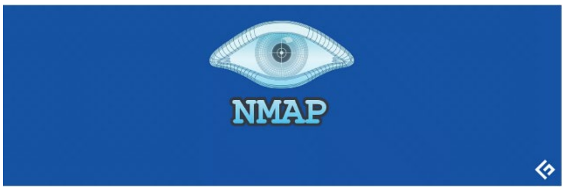
Burp Suite Enterprise Edition e Burp Suite Professional ed è l'arma preferita da oltre 70.000 utenti. Il motore crawl di Burp Scanner taglia ostacoli come i token CSRF, le funzionalità stateful e gli URL sovraccarichi o volatili. Inoltre, grazie al browser Chromium incorporato, è in grado di eseguire il rendering e il crawling anche delle applicazioni che richiedono l'uso di JavaScript, con le quali altri scanner di vulnerabilità web hanno difficoltà. Burp Scanner consente di risparmiare un'enorme quantità di tempo e di fatica sprecata. Burp Scanner utilizza tecniche di fingerprinting della posizione per identificare queste aree, riducendo drasticamente il numero di richieste effettuate durante i test.

Burp Suite

- **Nessus**: è uno dei più popolari scanner di vulnerabilità, con oltre due milioni di download in tutto il mondo. Nessus fornisce una buona valutazione delle vulnerabilità, aiuta a ridurre la superficie di attacco della propria organizzazione e a garantire la conformità. Lo scanner di vulnerabilità Nessus è dotato di funzionalità di rilevamento delle risorse ad alta velocità, verifica della configurazione, profilazione degli obiettivi, rilevamento del malware, rilevamento dei dati sensibili e altro ancora. Lo strumento Nessus supporta un numero maggiore di tecnologie rispetto alle soluzioni della concorrenza, scansionando sistemi operativi, dispositivi di rete, firewall di nuova generazione, hypervisor, database, server web e infrastrutture critiche alla ricerca di vulnerabilità, minacce e violazioni della conformità. Con la più grande libreria di controlli di vulnerabilità e configurazione continuamente aggiornata al mondo e il supporto del team di esperti di ricerca sulle vulnerabilità di Tenable, Nessus stabilisce lo standard per la velocità e l'accuratezza della scansione delle vulnerabilità. La versione Professional è ideale per consulenti, pen tester e professionisti della sicurezza, con la possibilità di scansionare un numero illimitato di IP e ottenere i risultati in tempo reale e la creazione di report personalizzati. In ogni caso, gli indirizzi IP o gli host da cui si esegue la scansione devono essere autorizzati. Questa versione non supporta la gestione dei dispositivi mobili.

Nessus
vulnerability scanner

- **Nmap**: Nmap, fornisce funzionalità open-source e per l'auditing dell'infrastruttura IT, come la scansione delle porte, la scoperta degli host o l'identificazione dei dispositivi in una rete. Sia i pen tester che gli attori delle minacce utilizzano Nmap per raccogliere informazioni sui loro obiettivi e Nmap è stato riconosciuto dal CISA come un importante strumento gratuito per la sicurezza delle reti. Le capacità di scansione delle vulnerabilità di Nmap si basano sugli script di rilevamento delle vulnerabilità classificati sotto "vuln" per le vulnerabilità o sugli script personalizzati. Gli utenti possono eseguire gli script integrati singolarmente o collettivamente utilizzando il comando "vuln". Inoltre, gli utenti possono anche scaricare script personalizzati come Vulscan o Vulners. Come per qualsiasi test di penetrazione o scansione di vulnerabilità, gli utenti devono tenere presente che queste scansioni invasive devono essere eseguite solo previa autorizzazione. Vuln e Vulners sono inclusi nel database degli script NSE di base e saranno aggiornati quando si aggiorneranno tutti gli script per Nmap.



- **OpenVAS**: È un framework di diversi servizi e strumenti che offre una soluzione di scansione / gestione delle vulnerabilità completa e potente. Le sue funzioni includono test non autenticati, test autenticati, vari protocolli Internet e industriali di alto e basso livello, ottimizzazione delle prestazioni per scansioni su larga scala e un potente linguaggio di programmazione interno per implementare qualsiasi tipo di test di vulnerabilità. Il progetto è nato nel 2005 come fork del celebre Nessus (commerciale), ed è rilasciato come OpenSource alla comunità sotto la licenza GNU General Public License (GNU GPL). È comunemente utilizzata dalle aziende come parte delle loro soluzioni di mitigazione per identificare rapidamente eventuali lacune nei server o nelle applicazioni di produzione o addirittura di sviluppo. Non si tratta di una soluzione definitiva, ma può aiutare a eliminare le vulnerabilità più comuni che potrebbero essere sfuggite al controllo. OpenVAS offre molte opzioni per il monitoraggio continuo e programmato e per la gestione delle vulnerabilità. Se si lavoro in un team o in una pipeline, questo può permettere di ottimizzare in modo efficiente e rapido le soluzioni attuali.

# Valutazione del rischio e mitigazione apportate

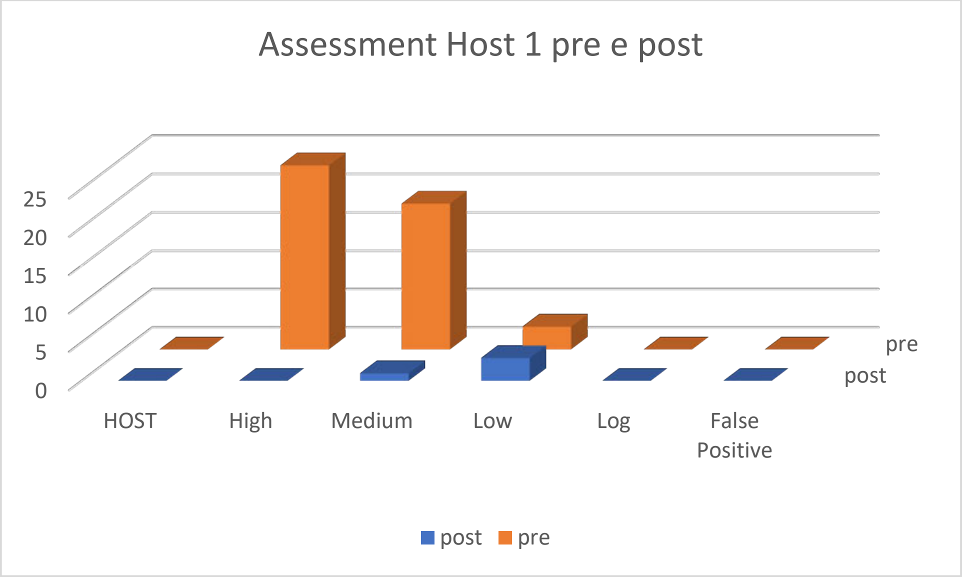
Il presente lavoro ha avuto come obiettivo il vulnerability assessment di tre host, relative a dimostratori di progetto, di cui sono stati indicati gli IP di accesso in rete. Questo tipo di analisi rientra nell'host assessment, perché rispetto al network assessment, consente di visualizzare con maggiore precisione le impostazioni di configurazione e quelle della cronologia delle patch. È stato utilizzato come tool di analisi OpenVAS.

L'analisi ha evidenziato sul primo host la presenza di numerose vulnerabilità relative a Grafana, applicazione web open source per la visualizzazione e l'analisi interattiva dei dati. Sui restanti host analizzati, come riportato nell'appendice, non sono stati rilevati vulnerabilità significative. I report generati sono stati consegnati al personale tecnico per valutare le possibili azioni di sanificazione delle vulnerabilità. Dopo che il personale tecnico ha provveduto ad eseguire operazioni di sanificazione, è stata rieseguita la scansione dei tre host per verificare se le vulnerabilità erano ancora presenti.

Di seguito vengono riportate per ogni host i risultati delle scansioni con il confronto pre e post sanificazione.

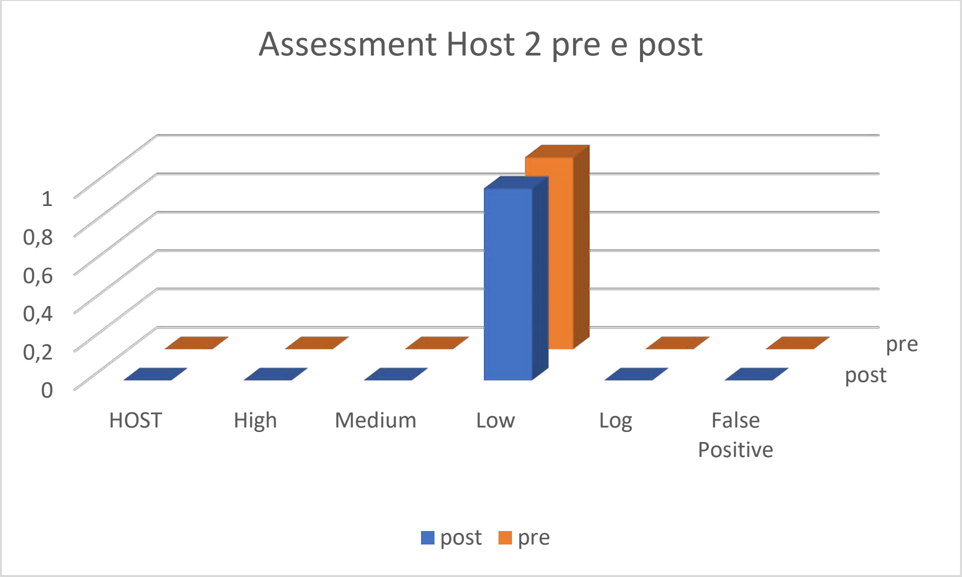
# HOST 1 analisi pre/post sanificazione

| | HOST | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|---|
| pre | a.a.a.xxx | 24 | 19 | 3 | 0 | 0 |
| post | a.a.a.xxx | 0 | 1 | 3 | 0 | 0 |



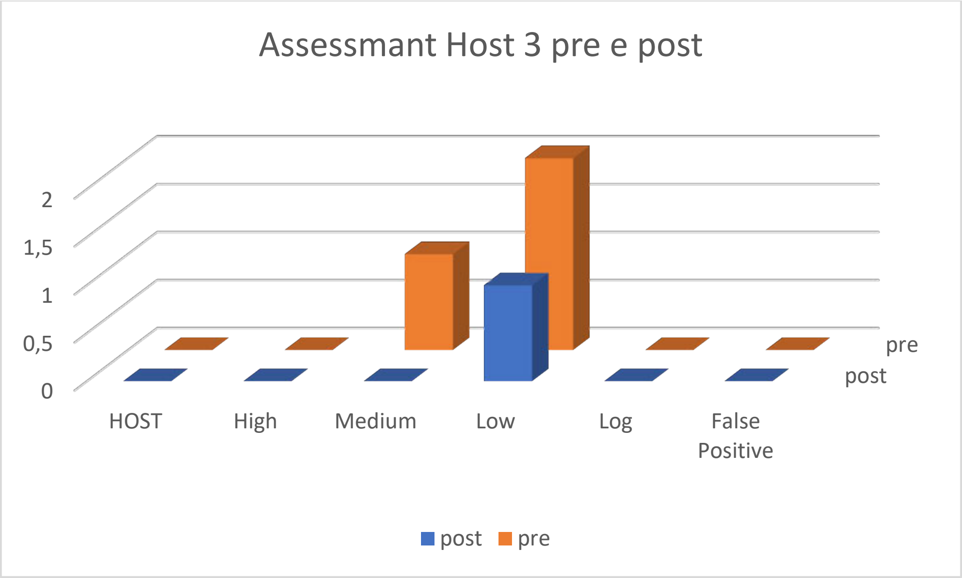
# HOST 2 analisi pre/post sanificazione

| | HOST | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|---|
| pre | a.a.a.yyy | 0 | 0 | 1 | 0 | 0 |
| post | a.a.a.yyy | 0 | 0 | 1 | 0 | 0 |



## HOST 3 analisi pre/post sanificazione

| | HOST | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|---|
| pre | a.a.a.zzz | 0 | 1 | 2 | 0 | 0 |
| post | a.a.a.zzz | 0 | 0 | 1 | 0 | 0 |



# Conclusioni

A seguito dell'analisi effettuata sui tre host, ove possibile sono state applicate tutte le patch necessarie, eseguendo l'aggiornamento delle versioni che presentavano vulnerabilità, come ad esempio Grafana per il primo host. I report hanno fornito suggerimenti utili a correggere le vulnerabilità riscontrate. Grazie agli questi, infatti, sono state corrette tutte le vulnerabilità gravi ed intermedie, e granparte di quelle leggere. Si suggerisce di continuare la ordinaria manutenzione trimestrale, ed una nuova valutazione del rischio approfondita ad un anno dalla presente.

# Appendice

Di seguito sono riportati i report generati durante i test.

# Scan Report

March 13, 2024

### Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “Immediate scan of IP `a.a.a.xxx` ”. The scan started at Wed Mar 13 13:39:25 2024 UTC and ended at Wed Mar 13 13:54:43 2024 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| a.a.a.xxx<br>xxxxxxxxxxxxxx.icar.cnr.it | 24 | 19 | 3 | 0 | 0 |
| Total: 1 | 24 | 19 | 3 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 46 results selected by the filtering described above. Before filtering there were 150 results.

# 2 Results per Host

## 2.1 a.a.a.xxx

Host scan start Wed Mar 13 13:39:47 2024 UTC
Host scan end

| Service (Port) | Threat Level |
|---|---|
| 3000/tcp | High |
| 443/tcp | High |
| 3000/tcp | Medium |
| 443/tcp | Medium |
| 111/tcp | Medium |
| general/tcp | Low |
| general/icmp | Low |
| 22/tcp | Low |

### 2.1.1 High 3000/tcp

High (CVSS: 9.8)

NVT: Grafana 6.3.0-beta1 < 8.5.16, 9.x < 9.2.8, 9.3.0 < 9.3.2 SAML Privilege Escalation Vulnerability (GHSA-5hcf-rqj9-xh96)

**Summary**
Grafana is prone to a privilege escalation vulnerability via SAML.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.5.16
Installation
path / port:       /
```

**Solution:**
**Solution type:** VendorFix
Update to version 8.5.16, 9.2.8, 9.3.2 or later.

**Affected Software/OS**
Grafana version 6.3.0-beta1 through 9.3.1.

**Vulnerability Insight**
Grafana Enterprise is using crewjam/saml library for SAML integration. On Nov 30, 2022 an advisory and relevant fix was published in the upstream library, which described a vulnerability allowing privilege escalation when processing SAML responses containing multiple assertions.
The vulnerability is possible to exploit only when a SAML document is not signed and multiple assertions are being used, where at least one assertion is signed. As a result, an attacker could intercept the SAML response and add any unsigned assertion, which would be parsed as signed by the library.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana 6.3.0-beta1 < 8.5.16, 9.x < 9.2.8, 9.3.0 < 9.3.2 SAML Privilege Escalat.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.149215
Version used: `2023-10-13T05:06:10Z`

**References**

```
cve: CVE-2022-41912
url: https://github.com/grafana/grafana/security/advisories/GHSA-5hcf-rqj9-xh96
cert-bund: WID-SEC-2023-0202
cert-bund: WID-SEC-2022-2338
dfn-cert: DFN-CERT-2023-1395
dfn-cert: DFN-CERT-2023-0323
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2023-0291
dfn-cert: DFN-CERT-2023-0044
dfn-cert: DFN-CERT-2023-0030
dfn-cert: DFN-CERT-2022-2864
```

High (CVSS: 9.8)

NVT: Grafana 6.7.x < 8.5.27, 9.x < 9.2.20, 9.3.x < 9.3.16, 9.4.x < 9.4.13, 9.5.x < 9.5.5, 10.x < 10.0.1 Authentication Bypass Vulnerability

**Summary**
Grafana is prone to an authentication bypass vulnerability.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.5.27
Installation
path / port:       /
```

**Solution:**
**Solution type:** VendorFix
Update to version 8.5.27, 9.2.20, 9.3.16, 9.4.13, 9.5.5, 10.0.1 or later.

**Affected Software/OS**
Grafana versions 6.7.x prior to 8.5.27, version 9.x prior to 9.2.20, 9.3.x prior to 9.3.16, 9.4.x prior to 9.4.13, 9.5.x prior to 9.5.5 and 10.x prior to 10.0.1.

**Vulnerability Insight**
Grafana validates Azure Active Directory accounts based on the email claim. On Azure AD, the profile email field is not unique across Azure AD tenants. This can enable a Grafana account takeover and authentication bypass when Azure AD OAuth is configured with a multi-tenant Azure AD OAuth application.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana 6.7.x < 8.5.27, 9.x < 9.2.20, 9.3.x < 9.3.16, 9.4.x < 9.4.13, 9.5.x < 9.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.124342
Version used: `2023-10-13T05:06:10Z`

**References**

```
cve: CVE-2023-3128
url: https://grafana.com/blog/2023/06/22/grafana-security-release-for-cve-2023-3
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪128/
cert-bund: WID-SEC-2023-1551
dfn-cert: DFN-CERT-2023-1676
dfn-cert: DFN-CERT-2023-1588
```

High (CVSS: 8.8)

NVT: Grafana CSRF Vulnerability (GHSA-cmf4-h3xc-jw8w)

**Summary**
Grafana is prone to a cross-site request forgery (CSRF) vulnerability.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     7.5.15
Installation
path / port:       /
```

**Solution:**
**Solution type:** VendorFix
Update to version 7.5.15, 8.3.5 or later.

**Affected Software/OS**
Grafana version 3.0-beta1 through 7.5.14 and 8.x through 8.3.4.

**Vulnerability Detection Method**
An attacker can exploit this vulnerability for privilege escalation by tricking an authenticated user into inviting the attacker as a new user with high privileges.
Details: Grafana CSRF Vulnerability (GHSA-cmf4-h3xc-jw8w)
OID:1.3.6.1.4.1.25623.1.0.147617
Version used: 2022-05-02T03:04:50Z

**References**

```
cve: CVE-2022-21703
url: https://github.com/grafana/grafana/security/advisories/GHSA-cmf4-h3xc-jw8w
cert-bund: WID-SEC-2022-0407
cert-bund: CB-K22/0159
dfn-cert: DFN-CERT-2022-2496
dfn-cert: DFN-CERT-2022-2397
dfn-cert: DFN-CERT-2022-2350
dfn-cert: DFN-CERT-2022-1386
dfn-cert: DFN-CERT-2022-0922
dfn-cert: DFN-CERT-2022-0794
```

High (CVSS: 8.5)

NVT: Grafana Datasource Network Restriction Bypass Vulnerability (GHSA-9rrr-6fq2-4f99)

**Summary**
Grafana is prone to a datasource network restriction bypass vulnerability.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     7.5.16
Installation
path / port:       /
```

**Impact**
The vulnerability is only impacting Grafana Enterprise when the 'Request security allow list' is used and there is a possibility to add a custom datasource to Grafana which returns HTTP redirects. In this scenario, Grafana would blindly follow the redirects and potentially give secure information to the clients.

**Solution:**
**Solution type:** VendorFix
Update to version 7.5.16, 8.5.3 or later.

**Affected Software/OS**
Grafana version 7.4.x through 7.5.15 and 8.x through 8.5.2.

**Vulnerability Insight**
In Grafana Enterprise, 'Request security allow list' allows to configure Grafana in a way so that the instance doesn't call or only calls specific hosts.
The vulnerability allows to bypass these security configurations if a malicious datasource (running on an allowed host) returns an HTTP redirect to a forbidden host.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana Datasource Network Restriction Bypass Vulnerability (GHSA-9rrr-6fq2-4f9.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.148162
Version used: `2022-06-03T10:57:19Z`

**References**

```
cve: CVE-2022-29170
url: https://github.com/grafana/grafana/security/advisories/GHSA-9rrr-6fq2-4f99
cert-bund: WID-SEC-2022-1907
cert-bund: CB-K22/0639
```

. . . continues on next page . . .

. . . continued from previous page . . .

dfn-cert: DFN-CERT-2022-2825

High (CVSS: 8.1)

NVT: Grafana Image Renderer Vulnerability (GHSA-2cfh-233g-m4c5)

**Summary**
Grafana is prone to a vulnerability in Grafana Image Renderer.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.3.11
Installation
path / port:       /
```

**Solution:**
**Solution type:** VendorFix
Update to version 8.3.11, 8.4.11, 8.5.11, 9.0.8, 9.1.2 or later.

**Affected Software/OS**
Grafana version 9.x and prior.

**Vulnerability Insight**
The Chromium browser embedded in the Grafana image renderer allows for 'printing' of unauthorized files in a PNG file. This makes it possible for a malicious user to retrieve unauthorized files under some network conditions or via a fake datasource (if the user has admin permissions in Grafana). This vulnerability permits unauthorized file disclosure and is a potential DoS vector through targeting of extremely large files.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana Image Renderer Vulnerability (GHSA-2cfh-233g-m4c5)`
OID:1.3.6.1.4.1.25623.1.0.148673
Version used: `2023-10-18T05:05:17Z`

**References**

```
cve: CVE-2022-31176
url: https://github.com/grafana/grafana-image-renderer/security/advisories/GHSA-
↪2cfh-233g-m4c5
cert-bund: WID-SEC-2022-1221
```

High (CVSS: 8.1)

NVT: Grafana < 8.5.15, 9 < 9.2.4 Multiple Vulnerabilities

**Summary**
Grafana is prone to multiple vulnerabilities.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.5.15
Installation
path / port:       /
```

**Solution:**
**Solution type:** VendorFix
Update to version 8.5.15, 9.2.4 or later.

**Affected Software/OS**
Grafana prior to version 8.5.15 and version 9 prior to 9.2.4.

**Vulnerability Insight**
The following vulnerabilities exist:
- CVE-2022-39306: Vulnerability makes it possible to use the invitation link to sign up with an arbitrary username/email with a malicious intent
- CVE-2022-39307: The impacted endpoint leaks information to unauthenticated users and introduces a security risk.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana < 8.5.15, 9 < 9.2.4 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.126208
Version used: `2023-10-18T05:05:17Z`

**References**

```
cve: CVE-2022-39306
cve: CVE-2022-39307
url: https://github.com/grafana/grafana/security/advisories/GHSA-2x6g-h2hg-rq84
url: https://github.com/grafana/grafana/security/advisories/GHSA-3p62-42x7-gxg5
cert-bund: WID-SEC-2023-0334
dfn-cert: DFN-CERT-2023-2756
dfn-cert: DFN-CERT-2023-1395
dfn-cert: DFN-CERT-2023-0322
```

High (CVSS: 7.8)

NVT: Grafana Privilege Escalation Vulnerability (GHSA-rhxj-gh46-jvw8)

**Summary**
Grafana is prone to a privilege escalation vulnerability.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.5.14
Installation
path / port:       /
```

**Impact**
An attacker can convince a server admin to download and successfully run a malicious plugin even though unsigned plugins are not allowed.

**Solution:**
**Solution type:** VendorFix
Update to version 8.5.14, 9.1.8 or later.

**Affected Software/OS**
Grafana version 7.x through 8.5.13, 9.x through 9.1.7.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana Privilege Escalation Vulnerability (GHSA-rhxj-gh46-jvw8)`
OID:1.3.6.1.4.1.25623.1.0.124200
Version used: `2023-10-18T05:05:17Z`

**References**

```
cve: CVE-2022-31123
url: https://github.com/grafana/grafana/security/advisories/GHSA-rhxj-gh46-jvw8
cert-bund: WID-SEC-2023-1022
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2022-1702
dfn-cert: DFN-CERT-2023-2756
dfn-cert: DFN-CERT-2023-1395
dfn-cert: DFN-CERT-2023-0322
```

High (CVSS: 7.5)

NVT: Grafana Privilege Escalation Vulnerability (GHSA-x744-mm8v-vpgr)

**Summary**
Grafana is prone to a privilege escalation vulnerability.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.5.14
Installation
path / port:       /
```

**Impact**
The destination plugin could receive a Grafana authentication cookie of the user.

**Solution:**
**Solution type:** VendorFix
Update to version 8.5.14, 9.1.8 or later.

**Affected Software/OS**
Grafana version 5.0.0-beta1 through 8.5.13, 9.x through 9.1.7.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana Privilege Escalation Vulnerability (GHSA-x744-mm8v-vpgr)`
OID:1.3.6.1.4.1.25623.1.0.124198
Version used: `2023-10-18T05:05:17Z`

**References**

```
cve: CVE-2022-39201
url: https://github.com/grafana/grafana/security/advisories/GHSA-x744-mm8v-vpgr
cert-bund: WID-SEC-2022-1702
dfn-cert: DFN-CERT-2023-2756
dfn-cert: DFN-CERT-2023-1395
dfn-cert: DFN-CERT-2023-0322
```

High (CVSS: 7.5)

NVT: Grafana 7.3.0-beta1 < 8.5.24, 9.x < 9.2.17, 9.3.x < 9.3.13, 9.4.x < 9.4.9 DoS Vulnerability

**Summary**

. . . continues on next page . . .

. . . continued from previous page . . .

Grafana is prone to a denial of service (DoS) vulnerability in the crewjam/saml library used for SAML integration.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.5.24
Installation
path / port:       /
```

**Impact**

The use of flate.NewReader in crewjam/saml does not limit the size of the input. The user could pass more than 1 MB of data in the HTTP request to the processing functions, which will be decompressed server-side using the Deflate algorithm. Therefore, after repeating the same request multiple times, it is possible to achieve a reliable crash since the operating system kills the process.

In Grafana Enterprise, SAML single logout is using the aforementioned functions. Therefore, it's impacted by the vulnerability.

**Solution:**

**Solution type:** VendorFix

- Update to version 8.5.24, 9.2.17, 9.3.13, 9.4.9 or later.
- As an alternative mitigation, disabling single logout in SAML or not using the SAML authentication entirely would mitigate the vulnerability.

**Affected Software/OS**

Grafana versions starting from 7.3.0-beta1 and prior to 8.5.24, 9.x prior to 9.2.17, 9.3.x prior to 9.3.13 and 9.4.x prior to 9.4.9.

**Vulnerability Insight**

Grafana is using crewjam/saml library for SAML integration. On March 23, an advisory and relevant fix was published in the upstream library, which described a vulnerability allowing denial of service attack.

**Vulnerability Detection Method**

Checks if a vulnerable version is present on the target host.

Details: `Grafana 7.3.0-beta1 < 8.5.24, 9.x < 9.2.17, 9.3.x < 9.3.13, 9.4.x < 9.4.9 DoS V.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.104715

Version used: `2023-10-13T05:06:10Z`

**References**

```
cve: CVE-2023-28119
url: https://grafana.com/blog/2023/04/26/grafana-security-release-new-versions-o
↪f-grafana-with-security-fixes-for-cve-2023-28119-and-cve-2023-1387/
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://github.com/advisories/GHSA-5mqj-xc49-246p
cert-bund: WID-SEC-2023-1088
```

High (CVSS: 7.5)

NVT: Grafana Privilege Escalation Vulnerability (GHSA-jv32-5578-pxjc)

**Summary**
Grafana is prone to a privilege escalation vulnerability.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.5.14
Installation
path / port:       /
```

**Impact**
The destination plugin could receive a Grafana authentication token of the user.

**Solution:**
**Solution type:** VendorFix
Update to version 8.5.14, 9.1.8 or later.

**Affected Software/OS**
Grafana version 7.x through 8.5.13, 9.x through 9.1.7.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana Privilege Escalation Vulnerability (GHSA-jv32-5578-pxjc)`
OID:1.3.6.1.4.1.25623.1.0.124199
Version used: `2023-10-18T05:05:17Z`

**References**

```
cve: CVE-2022-31130
url: https://github.com/grafana/grafana/security/advisories/GHSA-jv32-5578-pxjc
cert-bund: WID-SEC-2022-1702
dfn-cert: DFN-CERT-2023-2756
dfn-cert: DFN-CERT-2023-1395
dfn-cert: DFN-CERT-2023-0322
```

High (CVSS: 7.5)

NVT: Grafana OAuth Vulnerability (GHSA-mx47-6497-3fv2)

**Summary**
Grafana is prone to a vulnerability in OAuth.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.3.10
Installation
path / port:       /
```

**Impact**
It is possible for a malicious user who has authorization to log into a Grafana instance via a configured OAuth IdP to take over an existing Grafana account under some conditions.

**Solution:**
**Solution type:** VendorFix
Update to version 8.3.10, 8.4.10, 8.5.9, 9.0.3 or later.

**Affected Software/OS**
Grafana version 5.3 through 8.3.9, 8.4.x through 8.4.9, 8.5.x through 8.5.8 and 9.x through 9.0.2.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana OAuth Vulnerability (GHSA-mx47-6497-3fv2)`
OID:1.3.6.1.4.1.25623.1.0.148470
Version used: `2023-10-18T05:05:17Z`

**References**

```
cve: CVE-2022-31107
url: https://github.com/grafana/grafana/security/advisories/GHSA-mx47-6497-3fv2
cert-bund: WID-SEC-2022-1582
cert-bund: WID-SEC-2022-0696
dfn-cert: DFN-CERT-2023-1430
dfn-cert: DFN-CERT-2023-1395
dfn-cert: DFN-CERT-2022-2825
dfn-cert: DFN-CERT-2022-2397
dfn-cert: DFN-CERT-2022-2395
dfn-cert: DFN-CERT-2022-2394
dfn-cert: DFN-CERT-2022-2350
dfn-cert: DFN-CERT-2022-2163
dfn-cert: DFN-CERT-2022-1656
```

High (CVSS: 7.3)

NVT: Grafana 2.0.1 < 7.5.11, 8.x < 8.1.6 Snapshot Authentication Bypass Vulnerability (GHSA-69j6-29vr-p3j9)

**Summary**
Grafana is prone to an authentication bypass vulnerability in the snapshot functionality.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     7.5.11
Installation
path / port:       /
```

**Solution:**
**Solution type:** VendorFix
Update to version 7.5.11, 8.1.6 or later.

**Affected Software/OS**
Grafana version 2.0.1 through 7.5.10 and 8.x through 8.1.5.

**Vulnerability Insight**
Unauthenticated and authenticated users are able to view the snapshot with the lowest database key by accessing the literal paths:
/dashboard/snapshot/:key, or
/api/snapshots/:key
If the snapshot 'public_mode' configuration setting is set to true (vs default of false), unauthenticated users are able to delete the snapshot with the lowest database key by accessing the literal path:
/api/snapshots-delete/:deleteKey
Regardless of the snapshot 'public_mode' setting, authenticated users are able to delete the snapshot with the lowest database key by accessing the literal paths:
/api/snapshots/:key, or
/api/snapshots-delete/:deleteKey
The combination of deletion and viewing enables a complete walk through all snapshot data while resulting in complete snapshot data loss.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana 2.0.1 < 7.5.11, 8.x < 8.1.6 Snapshot Authentication Bypass Vulnerabilit.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.146863
Version used: `2022-09-14T10:57:19Z`

. . . continues on next page . . .

. . . continued from previous page . . .

**References**

```
cve: CVE-2021-39226
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://github.com/grafana/grafana/security/advisories/GHSA-69j6-29vr-p3j9
cert-bund: WID-SEC-2022-0401
cert-bund: CB-K21/1040
dfn-cert: DFN-CERT-2022-2121
dfn-cert: DFN-CERT-2022-2048
dfn-cert: DFN-CERT-2022-2003
dfn-cert: DFN-CERT-2022-1386
dfn-cert: DFN-CERT-2022-0922
dfn-cert: DFN-CERT-2022-0569
dfn-cert: DFN-CERT-2022-0152
dfn-cert: DFN-CERT-2021-2110
```

[ return to a.a.a.xxx ]

### 2.1.2 High 443/tcp

High (CVSS: 9.8)

NVT: Grafana 6.3.0-beta1 < 8.5.16, 9.x < 9.2.8, 9.3.0 < 9.3.2 SAML Privilege Escalation Vulnerability (GHSA-5hcf-rqj9-xh96)

**Summary**

Grafana is prone to a privilege escalation vulnerability via SAML.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.5.16
Installation
path / port:       /grafana
```

**Solution:**

**Solution type:** VendorFix

Update to version 8.5.16, 9.2.8, 9.3.2 or later.

**Affected Software/OS**

Grafana version 6.3.0-beta1 through 9.3.1.

**Vulnerability Insight**

. . . continues on next page . . .

. . . continued from previous page . . .

Grafana Enterprise is using crewjam/saml library for SAML integration. On Nov 30, 2022 an advisory and relevant fix was published in the upstream library, which described a vulnerability allowing privilege escalation when processing SAML responses containing multiple assertions.
The vulnerability is possible to exploit only when a SAML document is not signed and multiple assertions are being used, where at least one assertion is signed. As a result, an attacker could intercept the SAML response and add any unsigned assertion, which would be parsed as signed by the library.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana 6.3.0-beta1 < 8.5.16, 9.x < 9.2.8, 9.3.0 < 9.3.2 SAML Privilege Escalat.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.149215
Version used: `2023-10-13T05:06:10Z`

**References**

```
cve: CVE-2022-41912
url: https://github.com/grafana/grafana/security/advisories/GHSA-5hcf-rqj9-xh96
cert-bund: WID-SEC-2023-0202
cert-bund: WID-SEC-2022-2338
dfn-cert: DFN-CERT-2023-1395
dfn-cert: DFN-CERT-2023-0323
dfn-cert: DFN-CERT-2023-0291
dfn-cert: DFN-CERT-2023-0044
dfn-cert: DFN-CERT-2023-0030
dfn-cert: DFN-CERT-2022-2864
```

High (CVSS: 9.8)

NVT: Grafana 6.7.x < 8.5.27, 9.x < 9.2.20, 9.3.x < 9.3.16, 9.4.x < 9.4.13, 9.5.x < 9.5.5, 10.x < 10.0.1 Authentication Bypass Vulnerability

**Summary**
Grafana is prone to an authentication bypass vulnerability.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.5.27
Installation
path / port:       /grafana
```

**Solution:**
**Solution type:** VendorFix
Update to version 8.5.27, 9.2.20, 9.3.16, 9.4.13, 9.5.5, 10.0.1 or later.

. . . continues on next page . . .

. . . continued from previous page . . .

**Affected Software/OS**
Grafana versions 6.7.x prior to 8.5.27, version 9.x prior to 9.2.20, 9.3.x prior to 9.3.16, 9.4.x prior to 9.4.13, 9.5.x prior to 9.5.5 and 10.x prior to 10.0.1.

**Vulnerability Insight**
Grafana validates Azure Active Directory accounts based on the email claim. On Azure AD, the profile email field is not unique across Azure AD tenants. This can enable a Grafana account takeover and authentication bypass when Azure AD OAuth is configured with a multi-tenant Azure AD OAuth application.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana 6.7.x < 8.5.27, 9.x < 9.2.20, 9.3.x < 9.3.16, 9.4.x < 9.4.13, 9.5.x < 9.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.124342
Version used: `2023-10-13T05:06:10Z`

**References**
```
cve: CVE-2023-3128
url: https://grafana.com/blog/2023/06/22/grafana-security-release-for-cve-2023-3
↪128/
cert-bund: WID-SEC-2023-1551
dfn-cert: DFN-CERT-2023-1676
dfn-cert: DFN-CERT-2023-1588
```

High (CVSS: 8.8)

NVT: Grafana CSRF Vulnerability (GHSA-cmf4-h3xc-jw8w)

**Summary**
Grafana is prone to a cross-site request forgery (CSRF) vulnerability.

**Quality of Detection:** 80

**Vulnerability Detection Result**
```
Installed version: 7.5.4
Fixed version:     7.5.15
Installation
path / port:       /grafana
```

**Solution:**
**Solution type:** VendorFix
Update to version 7.5.15, 8.3.5 or later.

. . . continues on next page . . .

. . . continued from previous page . . .

**Affected Software/OS**
Grafana version 3.0-beta1 through 7.5.14 and 8.x through 8.3.4.

**Vulnerability Detection Method**
An attacker can exploit this vulnerability for privilege escalation by tricking an authenticated user into inviting the attacker as a new user with high privileges.
Details: `Grafana CSRF Vulnerability (GHSA-cmf4-h3xc-jw8w)`
OID:1.3.6.1.4.1.25623.1.0.147617
Version used: `2022-05-02T03:04:50Z`

**References**

```
cve: CVE-2022-21703
url: https://github.com/grafana/grafana/security/advisories/GHSA-cmf4-h3xc-jw8w
cert-bund: WID-SEC-2022-0407
cert-bund: CB-K22/0159
dfn-cert: DFN-CERT-2022-2496
dfn-cert: DFN-CERT-2022-2397
dfn-cert: DFN-CERT-2022-2350
dfn-cert: DFN-CERT-2022-1386
dfn-cert: DFN-CERT-2022-0922
dfn-cert: DFN-CERT-2022-0794
```

High (CVSS: 8.5)

NVT: Grafana Datasource Network Restriction Bypass Vulnerability (GHSA-9rrr-6fq2-4f99)

**Summary**
Grafana is prone to a datasource network restriction bypass vulnerability.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     7.5.16
Installation
path / port:       /grafana
```

**Impact**
The vulnerability is only impacting Grafana Enterprise when the 'Request security allow list' is used and there is a possibility to add a custom datasource to Grafana which returns HTTP redirects. In this scenario, Grafana would blindly follow the redirects and potentially give secure information to the clients.

**Solution:**

. . . continues on next page . . .

. . . continued from previous page . . .

**Solution type:** VendorFix
Update to version 7.5.16, 8.5.3 or later.

**Affected Software/OS**
Grafana version 7.4.x through 7.5.15 and 8.x through 8.5.2.

**Vulnerability Insight**
In Grafana Enterprise, 'Request security allow list' allows to configure Grafana in a way so that the instance doesn't call or only calls specific hosts.
The vulnerability allows to bypass these security configurations if a malicious datasource (running on an allowed host) returns an HTTP redirect to a forbidden host.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana Datasource Network Restriction Bypass Vulnerability (GHSA-9rrr-6fq2-4f9.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.148162
Version used: `2022-06-03T10:57:19Z`

**References**
```
cve: CVE-2022-29170
url: https://github.com/grafana/grafana/security/advisories/GHSA-9rrr-6fq2-4f99
cert-bund: WID-SEC-2022-1907
cert-bund: CB-K22/0639
dfn-cert: DFN-CERT-2022-2825
```

High (CVSS: 8.1)

NVT: Grafana Image Renderer Vulnerability (GHSA-2cfh-233g-m4c5)

**Summary**
Grafana is prone to a vulnerability in Grafana Image Renderer.

**Quality of Detection:** 80

**Vulnerability Detection Result**
```
Installed version: 7.5.4
Fixed version:     8.3.11
Installation
path / port:       /grafana
```

**Solution:**
**Solution type:** VendorFix
Update to version 8.3.11, 8.4.11, 8.5.11, 9.0.8, 9.1.2 or later.

. . . continues on next page . . .

. . . continued from previous page . . .

**Affected Software/OS**

Grafana version 9.x and prior.

**Vulnerability Insight**

The Chromium browser embedded in the Grafana image renderer allows for 'printing' of unauthorized files in a PNG file. This makes it possible for a malicious user to retrieve unauthorized files under some network conditions or via a fake datasource (if the user has admin permissions in Grafana). This vulnerability permits unauthorized file disclosure and is a potential DoS vector through targeting of extremely large files.

**Vulnerability Detection Method**

Checks if a vulnerable version is present on the target host.
Details: `Grafana Image Renderer Vulnerability (GHSA-2cfh-233g-m4c5)`
OID:1.3.6.1.4.1.25623.1.0.148673
Version used: `2023-10-18T05:05:17Z`

**References**

```
cve: CVE-2022-31176
url: https://github.com/grafana/grafana-image-renderer/security/advisories/GHSA-
↪2cfh-233g-m4c5
cert-bund: WID-SEC-2022-1221
```

High (CVSS: 8.1)

NVT: Grafana < 8.5.15, 9 < 9.2.4 Multiple Vulnerabilities

**Summary**

Grafana is prone to multiple vulnerabilities.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.5.15
Installation
path / port:       /grafana
```

**Solution:**

**Solution type:** VendorFix

Update to version 8.5.15, 9.2.4 or later.

**Affected Software/OS**

. . . continues on next page . . .

. . . continued from previous page . . .

Grafana prior to version 8.5.15 and version 9 prior to 9.2.4.

**Vulnerability Insight**

The following vulnerabilities exist:

- CVE-2022-39306: Vulnerability makes it possible to use the invitation link to sign up with an arbitrary username/email with a malicious intent
- CVE-2022-39307: The impacted endpoint leaks information to unauthenticated users and introduces a security risk.

**Vulnerability Detection Method**

Checks if a vulnerable version is present on the target host.

Details: `Grafana < 8.5.15, 9 < 9.2.4 Multiple Vulnerabilities`

OID:1.3.6.1.4.1.25623.1.0.126208

Version used: `2023-10-18T05:05:17Z`

**References**

```
cve: CVE-2022-39306
cve: CVE-2022-39307
url: https://github.com/grafana/grafana/security/advisories/GHSA-2x6g-h2hg-rq84
url: https://github.com/grafana/grafana/security/advisories/GHSA-3p62-42x7-gxg5
cert-bund: WID-SEC-2023-0334
dfn-cert: DFN-CERT-2023-2756
dfn-cert: DFN-CERT-2023-1395
dfn-cert: DFN-CERT-2023-0322
```

High (CVSS: 7.8)

NVT: Grafana Privilege Escalation Vulnerability (GHSA-rhxj-gh46-jvw8)

**Summary**

Grafana is prone to a privilege escalation vulnerability.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.5.14
Installation
path / port:       /grafana
```

**Impact**

An attacker can convince a server admin to download and successfully run a malicious plugin even though unsigned plugins are not allowed.

**Solution:**

**Solution type:** VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Update to version 8.5.14, 9.1.8 or later.

**Affected Software/OS**
Grafana version 7.x through 8.5.13, 9.x through 9.1.7.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana Privilege Escalation Vulnerability (GHSA-rhxj-gh46-jvw8)`
OID:1.3.6.1.4.1.25623.1.0.124200
Version used: `2023-10-18T05:05:17Z`

**References**

```
cve: CVE-2022-31123
url: https://github.com/grafana/grafana/security/advisories/GHSA-rhxj-gh46-jvw8
cert-bund: WID-SEC-2023-1022
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2022-1702
dfn-cert: DFN-CERT-2023-2756
dfn-cert: DFN-CERT-2023-1395
dfn-cert: DFN-CERT-2023-0322
```

High (CVSS: 7.5)

NVT: Grafana OAuth Vulnerability (GHSA-mx47-6497-3fv2)

**Summary**
Grafana is prone to a vulnerability in OAuth.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.3.10
Installation
path / port:       /grafana
```

**Impact**
It is possible for a malicious user who has authorization to log into a Grafana instance via a configured OAuth IdP to take over an existing Grafana account under some conditions.

**Solution:**
**Solution type:** VendorFix
Update to version 8.3.10, 8.4.10, 8.5.9, 9.0.3 or later.

. . . continues on next page . . .

. . . continued from previous page . . .

**Affected Software/OS**
Grafana version 5.3 through 8.3.9, 8.4.x through 8.4.9, 8.5.x through 8.5.8 and 9.x through 9.0.2.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana OAuth Vulnerability (GHSA-mx47-6497-3fv2)`
OID:1.3.6.1.4.1.25623.1.0.148470
Version used: `2023-10-18T05:05:17Z`

**References**

```
cve: CVE-2022-31107
url: https://github.com/grafana/grafana/security/advisories/GHSA-mx47-6497-3fv2
cert-bund: WID-SEC-2022-1582
cert-bund: WID-SEC-2022-0696
dfn-cert: DFN-CERT-2023-1430
dfn-cert: DFN-CERT-2023-1395
dfn-cert: DFN-CERT-2022-2825
dfn-cert: DFN-CERT-2022-2397
dfn-cert: DFN-CERT-2022-2395
dfn-cert: DFN-CERT-2022-2394
dfn-cert: DFN-CERT-2022-2350
dfn-cert: DFN-CERT-2022-2163
dfn-cert: DFN-CERT-2022-1656
```

High (CVSS: 7.5)

NVT: Grafana Privilege Escalation Vulnerability (GHSA-x744-mm8v-vpgr)

**Summary**
Grafana is prone to a privilege escalation vulnerability.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.5.14
Installation
path / port:       /grafana
```

**Impact**
The destination plugin could receive a Grafana authentication cookie of the user.

**Solution:**
**Solution type:** VendorFix
Update to version 8.5.14, 9.1.8 or later.

. . . continues on next page . . .

. . . continued from previous page . . .

**Affected Software/OS**
Grafana version 5.0.0-beta1 through 8.5.13, 9.x through 9.1.7.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana Privilege Escalation Vulnerability (GHSA-x744-mm8v-vpgr)`
OID:1.3.6.1.4.1.25623.1.0.124198
Version used: `2023-10-18T05:05:17Z`

**References**

```
cve: CVE-2022-39201
url: https://github.com/grafana/grafana/security/advisories/GHSA-x744-mm8v-vpgr
cert-bund: WID-SEC-2022-1702
dfn-cert: DFN-CERT-2023-2756
dfn-cert: DFN-CERT-2023-1395
dfn-cert: DFN-CERT-2023-0322
```

High (CVSS: 7.5)

NVT: Grafana Privilege Escalation Vulnerability (GHSA-jv32-5578-pxjc)

**Summary**
Grafana is prone to a privilege escalation vulnerability.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.5.14
Installation
path / port:       /grafana
```

**Impact**
The destination plugin could receive a Grafana authentication token of the user.

**Solution:**
**Solution type:** VendorFix
Update to version 8.5.14, 9.1.8 or later.

**Affected Software/OS**
Grafana version 7.x through 8.5.13, 9.x through 9.1.7.

**Vulnerability Detection Method**

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `Grafana Privilege Escalation Vulnerability (GHSA-jv32-5578-pxjc)`
OID:1.3.6.1.4.1.25623.1.0.124199
Version used: `2023-10-18T05:05:17Z`

**References**

```
cve: CVE-2022-31130
url: https://github.com/grafana/grafana/security/advisories/GHSA-jv32-5578-pxjc
cert-bund: WID-SEC-2022-1702
dfn-cert: DFN-CERT-2023-2756
dfn-cert: DFN-CERT-2023-1395
dfn-cert: DFN-CERT-2023-0322
```

High (CVSS: 7.5)

NVT: Grafana 7.3.0-beta1 < 8.5.24, 9.x < 9.2.17, 9.3.x < 9.3.13, 9.4.x < 9.4.9 DoS Vulnerability

**Summary**
Grafana is prone to a denial of service (DoS) vulnerability in the crewjam/saml library used for SAML integration.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.5.24
Installation
path / port:       /grafana
```

**Impact**
The use of flate.NewReader in crewjam/saml does not limit the size of the input. The user could pass more than 1 MB of data in the HTTP request to the processing functions, which will be decompressed server-side using the Deflate algorithm. Therefore, after repeating the same request multiple times, it is possible to achieve a reliable crash since the operating system kills the process.
In Grafana Enterprise, SAML single logout is using the aforementioned functions. Therefore, it's impacted by the vulnerability.

**Solution:**
**Solution type:** VendorFix
- Update to version 8.5.24, 9.2.17, 9.3.13, 9.4.9 or later.
- As an alternative mitigation, disabling single logout in SAML or not using the SAML authentication entirely would mitigate the vulnerability.

**Affected Software/OS**

. . . continues on next page . . .

. . . continued from previous page . . .

Grafana versions starting from 7.3.0-beta1 and prior to 8.5.24, 9.x prior to 9.2.17, 9.3.x prior to 9.3.13 and 9.4.x prior to 9.4.9.

**Vulnerability Insight**

Grafana is using crewjam/saml library for SAML integration. On March 23, an advisory and relevant fix was published in the upstream library, which described a vulnerability allowing denial of service attack.

**Vulnerability Detection Method**

Checks if a vulnerable version is present on the target host.

Details: `Grafana 7.3.0-beta1 < 8.5.24, 9.x < 9.2.17, 9.3.x < 9.3.13, 9.4.x < 9.4.9 DoS V.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.104715

Version used: `2023-10-13T05:06:10Z`

**References**

```
cve: CVE-2023-28119
url: https://grafana.com/blog/2023/04/26/grafana-security-release-new-versions-o
↪f-grafana-with-security-fixes-for-cve-2023-28119-and-cve-2023-1387/
url: https://github.com/advisories/GHSA-5mqj-xc49-246p
cert-bund: WID-SEC-2023-1088
```

High (CVSS: 7.3)

NVT: Grafana 2.0.1 < 7.5.11, 8.x < 8.1.6 Snapshot Authentication Bypass Vulnerability (GHSA-69j6-29vr-p3j9)

**Summary**

Grafana is prone to an authentication bypass vulnerability in the snapshot functionality.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     7.5.11
Installation
path / port:       /grafana
```

**Solution:**

**Solution type:** VendorFix

Update to version 7.5.11, 8.1.6 or later.

**Affected Software/OS**

Grafana version 2.0.1 through 7.5.10 and 8.x through 8.1.5.

. . . continues on next page . . .

. . . continued from previous page . . .

**Vulnerability Insight**

Unauthenticated and authenticated users are able to view the snapshot with the lowest database key by accessing the literal paths:
/dashboard/snapshot/:key, or
/api/snapshots/:key
If the snapshot 'public_mode' configuration setting is set to true (vs default of false), unauthenticated users are able to delete the snapshot with the lowest database key by accessing the literal path:
/api/snapshots-delete/:deleteKey
Regardless of the snapshot 'public_mode' setting, authenticated users are able to delete the snapshot with the lowest database key by accessing the literal paths:
/api/snapshots/:key, or
/api/snapshots-delete/:deleteKey
The combination of deletion and viewing enables a complete walk through all snapshot data while resulting in complete snapshot data loss.

**Vulnerability Detection Method**

Checks if a vulnerable version is present on the target host.
Details: `Grafana 2.0.1 < 7.5.11, 8.x < 8.1.6 Snapshot Authentication Bypass Vulnerabilit.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.146863
Version used: `2022-09-14T10:57:19Z`

**References**

```
cve: CVE-2021-39226
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://github.com/grafana/grafana/security/advisories/GHSA-69j6-29vr-p3j9
cert-bund: WID-SEC-2022-0401
cert-bund: CB-K21/1040
dfn-cert: DFN-CERT-2022-2121
dfn-cert: DFN-CERT-2022-2048
dfn-cert: DFN-CERT-2022-2003
dfn-cert: DFN-CERT-2022-1386
dfn-cert: DFN-CERT-2022-0922
dfn-cert: DFN-CERT-2022-0569
dfn-cert: DFN-CERT-2022-0152
dfn-cert: DFN-CERT-2021-2110
```

[ return to a.a.a.xxx ]

### 2.1.3 Medium 3000/tcp

Medium (CVSS: 6.6)

NVT: Grafana Privilege Escalation Vulnerability (GHSA-ff5c-938w-8c9q)

**Summary**
Grafana is prone to a privilege escalation vulnerability.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.5.13
Installation
path / port:       /
```

**Solution:**
**Solution type:** VendorFix
Update to version 8.5.13, 9.0.9, 9.1.6 or later.

**Affected Software/OS**
Grafana prior to version 8.5.13, version 9.0.x through 9.0.8 and 9.1.x through 9.1.5 if the Auth Proxy is used.

**Vulnerability Insight**
Grafana allows an escalation from Admin privileges to Server Admin when Auth proxy authentication is used.
Auth proxy allows to authenticate a user by only providing the username (or email) in a X-WEBAUTH-USER HTTP header: the trust assumption is that a front proxy will take care of authentication and that Grafana server is publicly reachable only with this front proxy.
Datasource proxy breaks this assumption:
- it is possible to configure a fake datasource pointing to a localhost Grafana install with a X-WEBAUTH-USER HTTP header containing admin username.
- This fake datasource can be called publicly via this proxying feature.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana Privilege Escalation Vulnerability (GHSA-ff5c-938w-8c9q)`
OID:1.3.6.1.4.1.25623.1.0.148743
Version used: `2023-10-18T05:05:17Z`

**References**

```
cve: CVE-2022-35957
url: https://github.com/grafana/grafana/security/advisories/GHSA-ff5c-938w-8c9q
cert-bund: WID-SEC-2022-1486
dfn-cert: DFN-CERT-2023-1430
dfn-cert: DFN-CERT-2023-1395
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2023-1045
dfn-cert: DFN-CERT-2022-2825
dfn-cert: DFN-CERT-2022-2350
```

Medium (CVSS: 6.4)

NVT: Grafana < 8.5.26, 9.x < 9.2.19, 9.3.x < 9.3.15, 9.4.x < 9.4.12, 9.5.0 < 9.5.3 Access Control Vulnerability

**Summary**
Grafana is prone to an access control vulnerability in the alert manager.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.5.26
Installation
path / port:       /
```

**Solution:**
**Solution type:** VendorFix
Update to version 8.5.26, 9.2.19, 9.3.15, 9.4.12, 9.5.3 or later.

**Affected Software/OS**
Grafana prior to version 8.5.26, version 9.x through 9.2.18, 9.3.x through 9.3.14, 9.4.x through 9.4.11 and version 9.5.x through 9.5.2.

**Vulnerability Insight**
The option to send a test alert is not available from the user panel UI for users having the Viewer role. It is still possible for a user with the Viewer role to send a test alert using the API as the API does not check access to this function. This might enable malicious users to abuse the functionality by sending multiple alert messages to e-mail and Slack, spamming users, prepare phishing attack or block SMTP server.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana < 8.5.26, 9.x < 9.2.19, 9.3.x < 9.3.15, 9.4.x < 9.4.12, 9.5.0 < 9.5.3 A.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.149749
Version used: `2023-10-13T05:06:10Z`

**References**

```
cve: CVE-2023-2183
url: https://grafana.com/security/security-advisories/cve-2023-2183/
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2023-1384
dfn-cert: DFN-CERT-2023-3124
dfn-cert: DFN-CERT-2023-1676
```

Medium (CVSS: 5.4)

NVT: Grafana < 8.5.21, 9.2.x < 9.2.13, 9.3.x < 9.3.8 Multiple Vulnerabilities

**Summary**
Grafana is prone to multiple vulnerabilities.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.5.21
Installation
path / port:       /
```

**Solution:**
**Solution type:** VendorFix
Update to version 8.5.21, 9.2.13, 9.3.8 or later.

**Affected Software/OS**
Grafana prior to version 8.5.21, version 9.2.0 through 9.2.12 and 9.3.0 through 9.3.7.

**Vulnerability Insight**
The following vulnerabilities exist:
- CVE-2023-0507: Stored XSS in geomap panel plugin via attribution
- CVE-2023-0594: Stored XSS in TraceView panel

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana < 8.5.21, 9.2.x < 9.2.13, 9.3.x < 9.3.8 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.149399
Version used: `2023-10-13T05:06:10Z`

**References**

```
cve: CVE-2023-0507
cve: CVE-2023-0594
url: https://grafana.com/blog/2023/02/28/grafana-security-release-new-versions-w
↪ith-security-fixes-for-cve-2023-0594-cve-2023-0507-and-cve-2023-22462/
cert-bund: WID-SEC-2023-0528
dfn-cert: DFN-CERT-2024-0349
dfn-cert: DFN-CERT-2023-0901
```

Medium (CVSS: 5.4)

NVT: Grafana XSS Vulnerability (GHSA-xc3p-28hw-q24g)

**Summary**
Grafana is prone to a cross-site scripting (XSS) vulnerability.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     7.5.15
Installation
path / port:       /
```

**Impact**
An attacker could serve HTML content through the Grafana datasource or plugin proxy and trick a user to visit this HTML page using a specially crafted link and execute an XSS attack. The attacker could either compromise an existing datasource for a specific Grafana instance or either set up its own public service and instruct anyone to set it up in their Grafana instance.

**Solution:**
**Solution type:** VendorFix
Update to version 7.5.15, 8.3.5 or later.

**Affected Software/OS**
Grafana version 2.0.0-beta1 through 8.3.4.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana XSS Vulnerability (GHSA-xc3p-28hw-q24g)`
OID:1.3.6.1.4.1.25623.1.0.147615
Version used: `2022-02-16T03:03:58Z`

**References**

```
cve: CVE-2022-21702
url: https://github.com/grafana/grafana/security/advisories/GHSA-xc3p-28hw-q24g
cert-bund: WID-SEC-2022-0407
cert-bund: CB-K22/0159
dfn-cert: DFN-CERT-2022-2496
dfn-cert: DFN-CERT-2022-2397
dfn-cert: DFN-CERT-2022-2350
dfn-cert: DFN-CERT-2022-1386
dfn-cert: DFN-CERT-2022-0922
dfn-cert: DFN-CERT-2022-0794
```

Medium (CVSS: 5.3)

NVT: Grafana < 9.4.12, 9.5.0 < 9.5.3 DoS Vulnerability

**Summary**
Grafana is prone to a denial of service (DoS) vulnerability.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     9.4.12
Installation
path / port:       /
```

**Solution:**
**Solution type:** VendorFix
Update to version 9.4.12, 9.5.3 or later.

**Affected Software/OS**
Grafana prior to version 9.4.12 and version 9.5.x through 9.5.2.

**Vulnerability Insight**
Using public dashboards users can query multiple distinct data sources using mixed queries. However such query has a possibility of crashing a Grafana instance. The only feature that uses mixed queries at the moment is public dashboards, but it's also possible to cause this by calling the query API directly. This might enable malicious users to crash Grafana instances through that endpoint.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana < 9.4.12, 9.5.0 < 9.5.3 DoS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.149748
Version used: `2023-10-13T05:06:10Z`

**References**

```
cve: CVE-2023-2801
url: https://grafana.com/security/security-advisories/cve-2023-2801/
cert-bund: WID-SEC-2023-1384
dfn-cert: DFN-CERT-2023-3124
dfn-cert: DFN-CERT-2023-1676
```

Medium (CVSS: 4.8)

NVT: Grafana < 8.5.22, 9.2.x < 9.2.15, 9.3.x < 9.3.11, 9.4.x < 9.4.7 XSS Vulnerability (GHSA-qrrg-gw7w-vp76)

**Summary**
Grafana is prone to a cross-site scripting (XSS) vulnerability.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.5.22
Installation
path / port:       /
```

**Solution:**
**Solution type:** VendorFix
Update to version 8.5.22, 9.2.15, 9.3.11, 9.4.7 or later.

**Affected Software/OS**
Grafana prior to version 8.5.22, 9.2.x prior to 9.2.15, 9.3.x prior to 9.3.11 and 9.4.x prior to 9.4.7.

**Vulnerability Insight**
The stored cross-site scripting (XSS) is possible due to improper sanitization of the Function Description value.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana < 8.5.22, 9.2.x < 9.2.15, 9.3.x < 9.3.11, 9.4.x < 9.4.7 XSS Vulnerabili.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.127372
Version used: `2023-10-13T05:06:10Z`

**References**

```
cve: CVE-2023-1410
url: https://github.com/grafana/bugbounty/security/advisories/GHSA-qrrg-gw7w-vp7
↪6
url: https://grafana.com/blog/2023/03/22/grafana-security-release-new-versions-w
↪ith-security-fixes-for-cve-2023-1410/
cert-bund: WID-SEC-2023-1130
cert-bund: WID-SEC-2023-0726
dfn-cert: DFN-CERT-2023-3124
dfn-cert: DFN-CERT-2023-1430
dfn-cert: DFN-CERT-2023-0999
dfn-cert: DFN-CERT-2023-0901
```

Medium (CVSS: 4.3)

NVT: Grafana IDOR Vulnerability (GHSA-63g3-9jq3-mccv)

**Summary**
Grafana is prone to an insecure direct object reference (IDOR) vulnerability on Grafana Teams APIs.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     7.5.15
Installation
path / port:       /
```

**Impact**
This vulnerability only impacts the following API endpoints:
- /teams/:teamId - an authenticated attacker can view unintended data by querying for the specific team ID.
- /teams/:search - an authenticated attacker can search for teams and see the total number of available teams, including for those teams that the user does not have access to.
- /teams/:teamId/members - when editors_can_admin flag is enabled, an authenticated attacker can see unintended data by querying for the specific team ID.

**Solution:**
**Solution type:** VendorFix
Update to version 7.5.15, 8.3.5 or later.

**Affected Software/OS**
Grafana version 5.0.0-beta1 through 7.5.14 and 8.x through 8.3.4.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana IDOR Vulnerability (GHSA-63g3-9jq3-mccv)`
OID:1.3.6.1.4.1.25623.1.0.147616
Version used: `2022-02-16T03:03:58Z`

**References**

```
cve: CVE-2022-21713
url: https://github.com/grafana/grafana/security/advisories/GHSA-63g3-9jq3-mccv
cert-bund: WID-SEC-2022-0407
cert-bund: CB-K22/0159
dfn-cert: DFN-CERT-2022-2496
dfn-cert: DFN-CERT-2022-2397
dfn-cert: DFN-CERT-2022-2350
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2022-1386
dfn-cert: DFN-CERT-2022-0922
dfn-cert: DFN-CERT-2022-0794
```

Medium (CVSS: 4.3)

NVT: Grafana 5.0.0 - 8.3.1 Directory Traversal Vulnerability

**Summary**
Grafana is prone to a directory traversal vulnerability for '.md' files.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     7.5.12
Installation
path / port:       /
```

**Solution:**
**Solution type:** VendorFix
Update to version 7.5.12, 8.3.2 or later.

**Affected Software/OS**
Grafana version 5.0.0 through 8.3.1.

**Vulnerability Insight**
Grafana contains a directory traversal vulnerability for fully lowercase or fully uppercase .md files. The vulnerability is limited in scope, and only allows access to files with the extension .md to authenticated users only.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana 5.0.0 - 8.3.1 Directory Traversal Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.147337
Version used: `2021-12-16T10:21:14Z`

**References**

```
cve: CVE-2021-43813
cve: CVE-2021-43815
url: https://github.com/grafana/grafana/security/advisories/GHSA-c3q8-26ph-9g2q
cert-bund: WID-SEC-2022-0405
cert-bund: CB-K21/1270
dfn-cert: DFN-CERT-2022-2825
dfn-cert: DFN-CERT-2022-2350
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2022-1790
dfn-cert: DFN-CERT-2022-1386
dfn-cert: DFN-CERT-2022-1142
dfn-cert: DFN-CERT-2022-1068
dfn-cert: DFN-CERT-2022-0922
dfn-cert: DFN-CERT-2022-0569
dfn-cert: DFN-CERT-2022-0152
dfn-cert: DFN-CERT-2022-0144
```

Medium (CVSS: 4.3)

NVT: Grafana OAuth Identity Token Vulnerability (GHSA-8wjh-59cw-9xh4)

**Summary**
Grafana is prone to a vulnerability in the OAuth identity token.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     7.5.13
Installation
path / port:       /
```

**Solution:**
**Solution type:** VendorFix
Update to version 7.5.13, 8.3.4 or later.

**Affected Software/OS**
Grafana version 7.2 through 7.5.12 and 8.x through 8.3.3.

**Vulnerability Insight**
When a data source has the Forward OAuth Identity feature enabled, sending a query to that datasource with an API token (and no other user credentials) will forward the OAuth Identity of the most recently logged-in user.
This can allow API token holders to retrieve data for which they may not have intended access.
All of the following must be true:
- The Grafana instance has data sources that support the Forward OAuth Identity feature. Graphite users, for example.
- The Grafana instance has a data source with the Forward OAuth Identity feature toggled on.
- The Grafana instance has OAuth enabled.
- The Grafana instance has usable API keys.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `Grafana OAuth Identity Token Vulnerability (GHSA-8wjh-59cw-9xh4)`
OID:1.3.6.1.4.1.25623.1.0.147463
Version used: `2022-01-27T12:34:58Z`

**References**

```
cve: CVE-2022-21673
url: https://github.com/grafana/grafana/security/advisories/GHSA-8wjh-59cw-9xh4
cert-bund: WID-SEC-2022-0406
cert-bund: CB-K22/0063
dfn-cert: DFN-CERT-2022-2496
dfn-cert: DFN-CERT-2022-2350
dfn-cert: DFN-CERT-2022-1790
dfn-cert: DFN-CERT-2022-1386
dfn-cert: DFN-CERT-2022-0922
dfn-cert: DFN-CERT-2022-0794
dfn-cert: DFN-CERT-2022-0569
```

[ return to a.a.a.xxx ]

### 2.1.4 Medium 443/tcp

Medium (CVSS: 6.6)

NVT: Grafana Privilege Escalation Vulnerability (GHSA-ff5c-938w-8c9q)

**Summary**
Grafana is prone to a privilege escalation vulnerability.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.5.13
Installation
path / port:       /grafana
```

**Solution:**
**Solution type:** VendorFix
Update to version 8.5.13, 9.0.9, 9.1.6 or later.

**Affected Software/OS**
Grafana prior to version 8.5.13, version 9.0.x through 9.0.8 and 9.1.x through 9.1.5 if the Auth Proxy is used.

. . . continues on next page . . .

. . . continued from previous page . . .

**Vulnerability Insight**

Grafana allows an escalation from Admin privileges to Server Admin when Auth proxy authentication is used.

Auth proxy allows to authenticate a user by only providing the username (or email) in a X-WEBAUTH-USER HTTP header: the trust assumption is that a front proxy will take care of authentication and that Grafana server is publicly reachable only with this front proxy.

Datasource proxy breaks this assumption:

- it is possible to configure a fake datasource pointing to a localhost Grafana install with a X-WEBAUTH-USER HTTP header containing admin username.
- This fake datasource can be called publicly via this proxying feature.

**Vulnerability Detection Method**

Checks if a vulnerable version is present on the target host.

Details: `Grafana Privilege Escalation Vulnerability (GHSA-ff5c-938w-8c9q)`

OID:1.3.6.1.4.1.25623.1.0.148743

Version used: `2023-10-18T05:05:17Z`

**References**

```
cve: CVE-2022-35957
url: https://github.com/grafana/grafana/security/advisories/GHSA-ff5c-938w-8c9q
cert-bund: WID-SEC-2022-1486
dfn-cert: DFN-CERT-2023-1430
dfn-cert: DFN-CERT-2023-1395
dfn-cert: DFN-CERT-2023-1045
dfn-cert: DFN-CERT-2022-2825
dfn-cert: DFN-CERT-2022-2350
```

Medium (CVSS: 6.4)

NVT: Grafana < 8.5.26, 9.x < 9.2.19, 9.3.x < 9.3.15, 9.4.x < 9.4.12, 9.5.0 < 9.5.3 Access Control Vulnerability

**Summary**

Grafana is prone to an access control vulnerability in the alert manager.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.5.26
Installation
path / port:       /grafana
```

**Solution:**

**Solution type:** VendorFix

Update to version 8.5.26, 9.2.19, 9.3.15, 9.4.12, 9.5.3 or later.

. . . continues on next page . . .

. . . continued from previous page . . .

**Affected Software/OS**
Grafana prior to version 8.5.26, version 9.x through 9.2.18, 9.3.x through 9.3.14, 9.4.x through 9.4.11 and version 9.5.x through 9.5.2.

**Vulnerability Insight**
The option to send a test alert is not available from the user panel UI for users having the Viewer role. It is still possible for a user with the Viewer role to send a test alert using the API as the API does not check access to this function. This might enable malicious users to abuse the functionality by sending multiple alert messages to e-mail and Slack, spamming users, prepare phishing attack or block SMTP server.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana < 8.5.26, 9.x < 9.2.19, 9.3.x < 9.3.15, 9.4.x < 9.4.12, 9.5.0 < 9.5.3 A.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.149749
Version used: `2023-10-13T05:06:10Z`

**References**

```
cve: CVE-2023-2183
url: https://grafana.com/security/security-advisories/cve-2023-2183/
cert-bund: WID-SEC-2023-1384
dfn-cert: DFN-CERT-2023-3124
dfn-cert: DFN-CERT-2023-1676
```

Medium (CVSS: 5.4)

NVT: Grafana < 8.5.21, 9.2.x < 9.2.13, 9.3.x < 9.3.8 Multiple Vulnerabilities

**Summary**
Grafana is prone to multiple vulnerabilities.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.5.21
Installation
path / port:       /grafana
```

**Solution:**
**Solution type:** VendorFix
Update to version 8.5.21, 9.2.13, 9.3.8 or later.

. . . continues on next page . . .

. . . continued from previous page . . .

**Affected Software/OS**
Grafana prior to version 8.5.21, version 9.2.0 through 9.2.12 and 9.3.0 through 9.3.7.

**Vulnerability Insight**
The following vulnerabilities exist:
- CVE-2023-0507: Stored XSS in geomap panel plugin via attribution
- CVE-2023-0594: Stored XSS in TraceView panel

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana < 8.5.21, 9.2.x < 9.2.13, 9.3.x < 9.3.8 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.149399
Version used: `2023-10-13T05:06:10Z`

**References**

```
cve: CVE-2023-0507
cve: CVE-2023-0594
url: https://grafana.com/blog/2023/02/28/grafana-security-release-new-versions-w
↪ith-security-fixes-for-cve-2023-0594-cve-2023-0507-and-cve-2023-22462/
cert-bund: WID-SEC-2023-0528
dfn-cert: DFN-CERT-2024-0349
dfn-cert: DFN-CERT-2023-0901
```

Medium (CVSS: 5.4)

NVT: Grafana XSS Vulnerability (GHSA-xc3p-28hw-q24g)

**Summary**
Grafana is prone to a cross-site scripting (XSS) vulnerability.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     7.5.15
Installation
path / port:       /grafana
```

**Impact**
An attacker could serve HTML content through the Grafana datasource or plugin proxy and trick a user to visit this HTML page using a specially crafted link and execute an XSS attack. The attacker could either compromise an existing datasource for a specific Grafana instance or either set up its own public service and instruct anyone to set it up in their Grafana instance.

. . . continues on next page . . .

. . . continued from previous page . . .

**Solution:**
**Solution type:** VendorFix
Update to version 7.5.15, 8.3.5 or later.

**Affected Software/OS**
Grafana version 2.0.0-beta1 through 8.3.4.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana XSS Vulnerability (GHSA-xc3p-28hw-q24g)`
OID:1.3.6.1.4.1.25623.1.0.147615
Version used: `2022-02-16T03:03:58Z`

**References**

```
cve: CVE-2022-21702
url: https://github.com/grafana/grafana/security/advisories/GHSA-xc3p-28hw-q24g
cert-bund: WID-SEC-2022-0407
cert-bund: CB-K22/0159
dfn-cert: DFN-CERT-2022-2496
dfn-cert: DFN-CERT-2022-2397
dfn-cert: DFN-CERT-2022-2350
dfn-cert: DFN-CERT-2022-1386
dfn-cert: DFN-CERT-2022-0922
dfn-cert: DFN-CERT-2022-0794
```

Medium (CVSS: 5.3)

NVT: Grafana < 9.4.12, 9.5.0 < 9.5.3 DoS Vulnerability

**Summary**
Grafana is prone to a denial of service (DoS) vulnerability.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     9.4.12
Installation
path / port:       /grafana
```

**Solution:**
**Solution type:** VendorFix
Update to version 9.4.12, 9.5.3 or later.

. . . continues on next page . . .

. . . continued from previous page . . .

**Affected Software/OS**
Grafana prior to version 9.4.12 and version 9.5.x through 9.5.2.

**Vulnerability Insight**
Using public dashboards users can query multiple distinct data sources using mixed queries. However such query has a possibility of crashing a Grafana instance. The only feature that uses mixed queries at the moment is public dashboards, but it's also possible to cause this by calling the query API directly. This might enable malicious users to crash Grafana instances through that endpoint.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana < 9.4.12, 9.5.0 < 9.5.3 DoS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.149748
Version used: `2023-10-13T05:06:10Z`

**References**

```
cve: CVE-2023-2801
url: https://grafana.com/security/security-advisories/cve-2023-2801/
cert-bund: WID-SEC-2023-1384
dfn-cert: DFN-CERT-2023-3124
dfn-cert: DFN-CERT-2023-1676
```

Medium (CVSS: 4.8)

NVT: Grafana < 8.5.22, 9.2.x < 9.2.15, 9.3.x < 9.3.11, 9.4.x < 9.4.7 XSS Vulnerability (GHSA-qrrg-gw7w-vp76)

**Summary**
Grafana is prone to a cross-site scripting (XSS) vulnerability.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     8.5.22
Installation
path / port:       /grafana
```

**Solution:**
**Solution type:** VendorFix
Update to version 8.5.22, 9.2.15, 9.3.11, 9.4.7 or later.

**Affected Software/OS**

. . . continues on next page . . .

. . . continued from previous page . . .

Grafana prior to version 8.5.22, 9.2.x prior to 9.2.15, 9.3.x prior to 9.3.11 and 9.4.x prior to 9.4.7.

**Vulnerability Insight**

The stored cross-site scripting (XSS) is possible due to improper sanitization of the Function Description value.

**Vulnerability Detection Method**

Checks if a vulnerable version is present on the target host.

Details: `Grafana < 8.5.22, 9.2.x < 9.2.15, 9.3.x < 9.3.11, 9.4.x < 9.4.7 XSS Vulnerabili.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.127372

Version used: `2023-10-13T05:06:10Z`

**References**

```
cve: CVE-2023-1410
url: https://github.com/grafana/bugbounty/security/advisories/GHSA-qrrg-gw7w-vp7
↪6
url: https://grafana.com/blog/2023/03/22/grafana-security-release-new-versions-w
↪ith-security-fixes-for-cve-2023-1410/
cert-bund: WID-SEC-2023-1130
cert-bund: WID-SEC-2023-0726
dfn-cert: DFN-CERT-2023-3124
dfn-cert: DFN-CERT-2023-1430
dfn-cert: DFN-CERT-2023-0999
dfn-cert: DFN-CERT-2023-0901
```

Medium (CVSS: 4.3)

NVT: Grafana OAuth Identity Token Vulnerability (GHSA-8wjh-59cw-9xh4)

**Summary**

Grafana is prone to a vulnerability in the OAuth identity token.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     7.5.13
Installation
path / port:       /grafana
```

**Solution:**

**Solution type:** VendorFix

Update to version 7.5.13, 8.3.4 or later.

. . . continues on next page . . .

. . . continued from previous page . . .

**Affected Software/OS**
Grafana version 7.2 through 7.5.12 and 8.x through 8.3.3.

**Vulnerability Insight**
When a data source has the Forward OAuth Identity feature enabled, sending a query to that datasource with an API token (and no other user credentials) will forward the OAuth Identity of the most recently logged-in user.
This can allow API token holders to retrieve data for which they may not have intended access.
All of the following must be true:
- The Grafana instance has data sources that support the Forward OAuth Identity feature. Graphite users, for example.
- The Grafana instance has a data source with the Forward OAuth Identity feature toggled on.
- The Grafana instance has OAuth enabled.
- The Grafana instance has usable API keys.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana OAuth Identity Token Vulnerability (GHSA-8wjh-59cw-9xh4)`
OID:1.3.6.1.4.1.25623.1.0.147463
Version used: `2022-01-27T12:34:58Z`

**References**
```
cve: CVE-2022-21673
url: https://github.com/grafana/grafana/security/advisories/GHSA-8wjh-59cw-9xh4
cert-bund: WID-SEC-2022-0406
cert-bund: CB-K22/0063
dfn-cert: DFN-CERT-2022-2496
dfn-cert: DFN-CERT-2022-2350
dfn-cert: DFN-CERT-2022-1790
dfn-cert: DFN-CERT-2022-1386
dfn-cert: DFN-CERT-2022-0922
dfn-cert: DFN-CERT-2022-0794
dfn-cert: DFN-CERT-2022-0569
```

Medium (CVSS: 4.3)

NVT: Grafana IDOR Vulnerability (GHSA-63g3-9jq3-mccv)

**Summary**
Grafana is prone to an insecure direct object reference (IDOR) vulnerability on Grafana Teams APIs.

**Quality of Detection:** 80

**Vulnerability Detection Result**
```
Installed version: 7.5.4
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:     7.5.15
Installation
path / port:       /grafana
```

**Impact**

This vulnerability only impacts the following API endpoints:
- /teams/:teamId - an authenticated attacker can view unintended data by querying for the specific team ID.
- /teams/:search - an authenticated attacker can search for teams and see the total number of available teams, including for those teams that the user does not have access to.
- /teams/:teamId/members - when editors_can_admin flag is enabled, an authenticated attacker can see unintended data by querying for the specific team ID.

**Solution:**

**Solution type:** VendorFix
Update to version 7.5.15, 8.3.5 or later.

**Affected Software/OS**

Grafana version 5.0.0-beta1 through 7.5.14 and 8.x through 8.3.4.

**Vulnerability Detection Method**

Checks if a vulnerable version is present on the target host.
Details: `Grafana IDOR Vulnerability (GHSA-63g3-9jq3-mccv)`
OID:1.3.6.1.4.1.25623.1.0.147616
Version used: `2022-02-16T03:03:58Z`

**References**

```
cve: CVE-2022-21713
url: https://github.com/grafana/grafana/security/advisories/GHSA-63g3-9jq3-mccv
cert-bund: WID-SEC-2022-0407
cert-bund: CB-K22/0159
dfn-cert: DFN-CERT-2022-2496
dfn-cert: DFN-CERT-2022-2397
dfn-cert: DFN-CERT-2022-2350
dfn-cert: DFN-CERT-2022-1386
dfn-cert: DFN-CERT-2022-0922
dfn-cert: DFN-CERT-2022-0794
```

Medium (CVSS: 4.3)

NVT: Grafana 5.0.0 - 8.3.1 Directory Traversal Vulnerability

**Summary**

Grafana is prone to a directory traversal vulnerability for '.md' files.

. . . continues on next page . . .

. . . continued from previous page . . .

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
Installed version: 7.5.4
Fixed version:     7.5.12
Installation
path / port:       /grafana
```

**Solution:**
**Solution type:** VendorFix
Update to version 7.5.12, 8.3.2 or later.

**Affected Software/OS**
Grafana version 5.0.0 through 8.3.1.

**Vulnerability Insight**
Grafana contains a directory traversal vulnerability for fully lowercase or fully uppercase .md files. The vulnerability is limited in scope, and only allows access to files with the extension .md to authenticated users only.

**Vulnerability Detection Method**
Checks if a vulnerable version is present on the target host.
Details: `Grafana 5.0.0 - 8.3.1 Directory Traversal Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.147337
Version used: `2021-12-16T10:21:14Z`

**References**

```
cve: CVE-2021-43813
cve: CVE-2021-43815
url: https://github.com/grafana/grafana/security/advisories/GHSA-c3q8-26ph-9g2q
cert-bund: WID-SEC-2022-0405
cert-bund: CB-K21/1270
dfn-cert: DFN-CERT-2022-2825
dfn-cert: DFN-CERT-2022-2350
dfn-cert: DFN-CERT-2022-1790
dfn-cert: DFN-CERT-2022-1386
dfn-cert: DFN-CERT-2022-1142
dfn-cert: DFN-CERT-2022-1068
dfn-cert: DFN-CERT-2022-0922
dfn-cert: DFN-CERT-2022-0569
dfn-cert: DFN-CERT-2022-0152
dfn-cert: DFN-CERT-2022-0144
```

[ return to a.a.a.xxx ]

### 2.1.5 Medium 111/tcp

Medium (CVSS: 6.4)

NVT: RPC Portmapper Service Public WAN (Internet) / Public LAN Accessible

**Product detection result**

```
cpe:/a:portmap:portmap
Detected by RPC Portmapper Service Detection (TCP) (OID: 1.3.6.1.4.1.25623.1.0.1
↪08090)
```

**Summary**

The script checks if the target host is running a RPC Portmapper service accessible from a public WAN (Internet) / public LAN.

**Quality of Detection:** 80

**Vulnerability Detection Result**

Vulnerability was detected according to the Vulnerability Detection Method.

**Solution:**

**Solution type:** Mitigation

- Only allow access to the RPC Portmapper service from trusted sources
- Disable the service if unused / not required

**Vulnerability Insight**

A public accessible RPC Portmapper service is generally seen as / assumed to be a security misconfiguration.

In addition openly accessible RPC Portmapper services can be abused for distributed denial of service (DDoS) reflection attacks against third parties.

Please see the references for more information.

**Vulnerability Detection Method**

Evaluate if the target host is running a RPC Portmapper service accessible from a public WAN (Internet) / public LAN.

Note: A configuration option 'Network type' to define if a scanned network should be seen as a public LAN can be found in the preferences of the following VT:

Global variable settings (OID: 1.3.6.1.4.1.25623.1.0.12288)

Details: `RPC Portmapper Service Public WAN (Internet) / Public LAN Accessible`

OID:1.3.6.1.4.1.25623.1.0.104901

Version used: `2023-09-13T05:05:22Z`

**Product Detection Result**

Product: `cpe:/a:portmap:portmap`

Method: `RPC Portmapper Service Detection (TCP)`

OID: 1.3.6.1.4.1.25623.1.0.108090)

. . . continues on next page . . .

. . . continued from previous page . . .

**References**

```
url: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sich
↪erheitslage/Reaktion/CERT-Bund/CERT-Bund-Reports/HowTo/Offene-Portmapper-Diens
↪te/Offene-Portmapper-Dienste.html
url: https://www.debian.org/doc/manuals/securing-debian-manual/rpc.en.html
url: https://blog.lumen.com/a-new-ddos-reflection-attack-portmapper-an-early-war
↪ning-to-the-industry/
```

[ return to a.a.a.xxx ]

### 2.1.6 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

**Summary**
The remote host implements TCP timestamps and therefore allows to compute the uptime.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 4287571699
Packet 2: 4287572775
```

**Impact**
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

**Solution:**
**Solution type:** Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'
Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

**Affected Software/OS**
TCP implementations that implement RFC1323/RFC7323.

. . . continues on next page . . .

. . . continued from previous page . . .

**Vulnerability Insight**
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

**Vulnerability Detection Method**
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP Timestamps Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-12-15T16:10:08Z`

**References**

```
url: https://datatracker.ietf.org/doc/html/rfc1323
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090
```

[ return to a.a.a.xxx ]

### 2.1.7 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

**Summary**
The remote host responded to an ICMP timestamp request.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

**Impact**
This information could theoretically be used to exploit weak time-based random number generators in other services.

**Solution:**
**Solution type:** Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely

. . . continues on next page . . .

. . . continued from previous page . . .

- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

**Vulnerability Insight**

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

**Vulnerability Detection Method**

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

Details: `ICMP Timestamp Reply Information Disclosure`

OID:1.3.6.1.4.1.25623.1.0.103190

Version used: `2023-05-11T09:09:33Z`

**References**

```
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[ return to a.a.a.xxx ]

### 2.1.8 Low 22/tcp

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

**Summary**

The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
umac-64@openssh.com
```

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm

Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2023-10-12T05:05:32Z`

**References**
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[ return to a.a.a.xxx ]

This file was automatically generated.

# Scan Report

March 13, 2024

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “Immediate scan of IP `a.a.a.yyy` ”. The scan started at Wed Mar 13 13:18:14 2024 UTC and ended at Wed Mar 13 14:25:04 2024 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| a.a.a.yyy | 0 | 0 | 1 | 0 | 0 |
| Total: 1 | 0 | 0 | 1 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level “Log” are not shown.
Issues with the threat level “Debug” are not shown.
Issues with the threat level “False Positive” are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains result 1 of the 1 results selected by the filtering above. Before filtering there were 10 results.

# 2 Results per Host

## 2.1 a.a.a.yyy

| | |
|---|---|
| Host scan start | Wed Mar 13 13:18:37 2024 UTC |
| Host scan end | Wed Mar 13 14:25:00 2024 UTC |

| Service (Port) | Threat Level |
|---|---|
| general/icmp | Low |

### 2.1.1 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

**Summary**
The remote host responded to an ICMP timestamp request.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
The following response / ICMP packet has been received:
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
- ICMP Type: 14
- ICMP Code: 0
```

**Impact**
This information could theoretically be used to exploit weak time-based random number generators in other services.

**Solution:**
**Solution type:** Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

**Vulnerability Insight**
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

**Vulnerability Detection Method**
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2023-05-11T09:09:33Z`

**References**
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658

[ return to a.a.a.yyy ]

# Scan Report

March 13, 2024

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “Immediate scan of IP `a.a.a.zzz` ”. The scan started at Wed Mar 13 13:39:35 2024 UTC and ended at Wed Mar 13 13:59:55 2024 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| a.a.a.zzz | 0 | 1 | 2 | 0 | 0 |
| Total: 1 | 0 | 1 | 2 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 3 results selected by the filtering described above. Before filtering there were 18 results.

# 2 Results per Host

## 2.1 a.a.a.zzz

Host scan start Wed Mar 13 13:39:56 2024 UTC
Host scan end Wed Mar 13 13:59:50 2024 UTC

| Service (Port) | Threat Level |
|---|---|
| 1883/tcp | Medium |
| general/tcp | Low |
| general/icmp | Low |

### 2.1.1 Medium 1883/tcp

Medium (CVSS: 6.4)

NVT: MQTT Broker Does Not Require Authentication

**Summary**
The remote MQTT broker does not require authentication.

**Quality of Detection:** 80

. . . continues on next page . . .

. . . continued from previous page . . .

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Solution:**
**Solution type:** Mitigation
Enable authentication.

**Vulnerability Detection Method**
Checks if authentication is required for the remote MQTT broker.
Details: `MQTT Broker Does Not Require Authentication`
OID:1.3.6.1.4.1.25623.1.0.140167
Version used: `2022-07-11T10:16:03Z`

**References**

```
url: https://www.heise.de/newsticker/meldung/MQTT-Protokoll-IoT-Kommunikation-vo
↪n-Reaktoren-und-Gefaengnissen-oeffentlich-einsehbar-3629650.html
```

[ return to a.a.a.zzz ]

### 2.1.2 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

**Summary**
The remote host implements TCP timestamps and therefore allows to compute the uptime.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 357303127
Packet 2: 357304182
```

**Impact**
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

**Solution:**
**Solution type:** Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

. . . continues on next page . . .

... continued from previous page ...

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'
Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

**Affected Software/OS**
TCP implementations that implement RFC1323/RFC7323.

**Vulnerability Insight**
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

**Vulnerability Detection Method**
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP Timestamps Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-12-15T16:10:08Z`

**References**

```
url: https://datatracker.ietf.org/doc/html/rfc1323
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090
```

[ return to a.a.a.zzz ]

### 2.1.3 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

**Summary**
The remote host responded to an ICMP timestamp request.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

... continues on next page ...

. . . continued from previous page . . .

**Impact**

This information could theoretically be used to exploit weak time-based random number generators in other services.

**Solution:**

**Solution type:** Mitigation

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

**Vulnerability Insight**

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

**Vulnerability Detection Method**

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2023-05-11T09:09:33Z`

**References**

```
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[ return to a.a.a.zzz ]

This file was automatically generated.

# Scan Report

April 17, 2024

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “Immediate scan of IP `a.a.a.xxx`    ”. The scan started at Wed Apr 17 14:37:14 2024 UTC and ended at Wed Apr 17 14:51:14 2024 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| a.a.a.xxx<br>xxxxxxxxxxxxxx.icar.cnr.it | 0 | 1 | 3 | 0 | 0 |
| Total: 1 | 0 | 1 | 3 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level “Log” are not shown.
Issues with the threat level “Debug” are not shown.
Issues with the threat level “False Positive” are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 4 results selected by the filtering described above. Before filtering there were 85 results.

# 2 Results per Host

## 2.1 a.a.a.xxx

Host scan start Wed Apr 17 14:37:36 2024 UTC
Host scan end Wed Apr 17 14:51:09 2024 UTC

| Service (Port) | Threat Level |
|---|---|
| 111/tcp | Medium |
| general/icmp | Low |
| general/tcp | Low |
| 22/tcp | Low |

### 2.1.1 Medium 111/tcp

Medium (CVSS: 6.4)

NVT: RPC Portmapper Service Public WAN (Internet) / Public LAN Accessible

**Product detection result**

```
cpe:/a:portmap:portmap
Detected by RPC Portmapper Service Detection (TCP) (OID: 1.3.6.1.4.1.25623.1.0.1
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪08090)
```

**Summary**
The script checks if the target host is running a RPC Portmapper service accessible from a public WAN (Internet) / public LAN.

**Quality of Detection:** 80

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Solution:**
**Solution type:** Mitigation
- Only allow access to the RPC Portmapper service from trusted sources
- Disable the service if unused / not required

**Vulnerability Insight**
A public accessible RPC Portmapper service is generally seen as / assumed to be a security misconfiguration.
In addition openly accessible RPC Portmapper services can be abused for distributed denial of service (DDoS) reflection attacks against third parties.
Please see the references for more information.

**Vulnerability Detection Method**
Evaluate if the target host is running a RPC Portmapper service accessible from a public WAN (Internet) / public LAN.
Note: A configuration option 'Network type' to define if a scanned network should be seen as a public LAN can be found in the preferences of the following VT:
Global variable settings (OID: 1.3.6.1.4.1.25623.1.0.12288)
Details: `RPC Portmapper Service Public WAN (Internet) / Public LAN Accessible`
OID:1.3.6.1.4.1.25623.1.0.104901
Version used: `2023-09-13T05:05:22Z`

**Product Detection Result**
Product: `cpe:/a:portmap:portmap`
Method: `RPC Portmapper Service Detection (TCP)`
OID: 1.3.6.1.4.1.25623.1.0.108090)

**References**

```
url: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sich
↪erheitslage/Reaktion/CERT-Bund/CERT-Bund-Reports/HowTo/Offene-Portmapper-Diens
↪te/Offene-Portmapper-Dienste.html
url: https://www.debian.org/doc/manuals/securing-debian-manual/rpc.en.html
url: https://blog.lumen.com/a-new-ddos-reflection-attack-portmapper-an-early-war
```

. . . continues on next page . . .

. . . continued from previous page . . .

↪ning-to-the-industry/

[ return to a.a.a.xxx ]

### 2.1.2 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

**Summary**

The remote host responded to an ICMP timestamp request.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

**Impact**

This information could theoretically be used to exploit weak time-based random number generators in other services.

**Solution:**

**Solution type:** Mitigation

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely

- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

**Vulnerability Insight**

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

**Vulnerability Detection Method**

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

Details: `ICMP Timestamp Reply Information Disclosure`

OID:1.3.6.1.4.1.25623.1.0.103190

Version used: `2023-05-11T09:09:33Z`

**References**

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[ return to a.a.a.xxx ]

### 2.1.3 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

**Summary**
The remote host implements TCP timestamps and therefore allows to compute the uptime.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 1994174984
Packet 2: 1994176070
```

**Impact**
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

**Solution:**
**Solution type:** Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'
Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

**Affected Software/OS**
TCP implementations that implement RFC1323/RFC7323.

**Vulnerability Insight**

... continues on next page ...

. . . continued from previous page . . .

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

**Vulnerability Detection Method**

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

Details: `TCP Timestamps Information Disclosure`

OID:1.3.6.1.4.1.25623.1.0.80091

Version used: `2023-12-15T16:10:08Z`

**References**

```
url: https://datatracker.ietf.org/doc/html/rfc1323
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090
```

[ return to a.a.a.xxx ]

### 2.1.4 Low 22/tcp

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

**Summary**

The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
```

**Solution:**

**Solution type:** Mitigation

Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**

. . . continues on next page . . .

. . . continued from previous page . . .

Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm

Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2023-10-12T05:05:32Z`

**References**

url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[ return to a.a.a.xxx ]

This file was automatically generated.

# Scan Report

April 17, 2024

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Immediate scan of IP `a.a.a.yyy` ". The scan started at Wed Apr 17 15:35:05 2024 UTC and ended at Wed Apr 17 15:58:54 2024 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| a.a.a.yyy | 0 | 0 | 1 | 0 | 0 |
| Total: 1 | 0 | 0 | 1 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level “Log” are not shown.
Issues with the threat level “Debug” are not shown.
Issues with the threat level “False Positive” are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains result 1 of the 1 results selected by the filtering above. Before filtering there were 11 results.

# 2 Results per Host

## 2.1 a.a.a.yyy

| | |
|---|---|
| Host scan start | Wed Apr 17 15:35:27 2024 UTC |
| Host scan end | Wed Apr 17 15:58:48 2024 UTC |

| Service (Port) | Threat Level |
|---|---|
| general/icmp | Low |

### 2.1.1 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

**Summary**
The remote host responded to an ICMP timestamp request.

**Quality of Detection:** 80

**Vulnerability Detection Result**

```
The following response / ICMP packet has been received:
```

. . . continues on next page . . .

... continued from previous page ...

```
- ICMP Type: 14
- ICMP Code: 0
```

**Impact**

This information could theoretically be used to exploit weak time-based random number generators in other services.

**Solution:**

**Solution type:** Mitigation

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

**Vulnerability Insight**

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

**Vulnerability Detection Method**

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2023-05-11T09:09:33Z`

**References**

```
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[ return to a.a.a.yyy ]

This file was automatically generated.

# Scan Report

April 17, 2024

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “Immediate scan of IP `a.a.a.zzz` ”. The scan started at Wed Apr 17 14:36:54 2024 UTC and ended at Wed Apr 17 14:56:32 2024 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

# 1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| a.a.a.zzz | 0 | 0 | 1 | 0 | 0 |
| Total: 1 | 0 | 0 | 1 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level “Log” are not shown.
Issues with the threat level “Debug” are not shown.
Issues with the threat level “False Positive” are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains result 1 of the 1 results selected by the filtering above. Before filtering there were 15 results.

# 2 Results per Host

## 2.1 a.a.a.zzz

| | |
|---|---|
| Host scan start | Wed Apr 17 14:37:16 2024 UTC |
| Host scan end | Wed Apr 17 14:56:27 2024 UTC |

| Service (Port) | Threat Level |
|---|---|
| general/icmp | Low |

### 2.1.1 Low general/icmp

| Low (CVSS: 2.1)<br>NVT: ICMP Timestamp Reply Information Disclosure |
|---|
| **Summary**<br>The remote host responded to an ICMP timestamp request. |
| **Quality of Detection:** 80 |
| **Vulnerability Detection Result**<br>The following response / ICMP packet has been received: |

. . . continues on next page . . .

. . . continued from previous page . . .

```
- ICMP Type: 14
- ICMP Code: 0
```

**Impact**
This information could theoretically be used to exploit weak time-based random number generators in other services.

**Solution:**
**Solution type:** Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

**Vulnerability Insight**
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

**Vulnerability Detection Method**
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2023-05-11T09:09:33Z`

**References**
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658

[ return to a.a.a.zzz ]