Università degli Studi di Salerno

Penetration Testing Report

ICLEAN

Antonio Allocca | Corso di PTEH | A.A. 2023/2024

UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Sommario

Executive Summary

L'attività di penetration testing condotta dallo studente Antonio Allocca nell'anno 2024 commissionato dal corso di Penetration Testing and Ethical Hacking sull'asset **iClean** dell'azienda **Hack The Box** è stata condotta per evidenziare gli aspetti critici del sistema e per poter studiare delle difese efficaci per contrastare gli attacchi che potrebbero verificarsi.
L'obiettivo principale del presente lavoro è stato quello di identificare, analizzare, sfruttare e documentare il maggior numero possibile di vulnerabilità all'interno del sistema esaminato. In particolare, si è puntato ad individuare le debolezze che potessero essere utilizzate per ottenere accesso non autorizzato ai file critici, come user.txt e root.txt.
Questo processo ha comportato un'analisi approfondita delle configurazioni di sicurezza, l'uso di strumenti specifici per la rilevazione delle vulnerabilità e l'applicazione di tecniche di exploit per verificare la reale possibilità di compromissione del sistema.
Ogni vulnerabilità scoperta è stata dettagliatamente documentata, descrivendo il

metodo di identificazione, l'approccio sfruttato per l'attacco e le misure suggerite per mitigare tali rischi in futuro.

Il testing è stato effettuato in **full black box** in quanto non sono stati forniti, da parte dell'azienda, dettagli sull'implementazione dell'asset ed eventuali risultati di testing precedenti.

I risultati ottenuti non sono rassicuranti in quanto sono state individuate svariate vulnerabilità talvolta critiche del sistema dovute ad una mancanza di aggiornamenti del sistema e all'assenza di opportune difese software che possono portare ad una compromissione totale della triade **CIA** (**C**onfidentiality, **I**ntegrity, and **A**vailability).

Dell'asset analizzato ne sono state riportate tutte le vulnerabilità in modo sia descrittivo che dettagliato spiegando le criticità di tali vulnerabilità. Oltre che alle vulnerabilità, sono state riportate anche le mitigazioni che potrebbero mitigare il rischio che l'asset venga compromesso.

Il rischio di essere compromessi è molto alto. Engagement Highlights

Tenendo conto che non sono stati posti limiti sulle tecniche e sugli strumenti utilizzabili durante l'attività di testing, durante il processo di testing durato all'incirca un mese, e considerati gli obiettivi del processo, ovvero verificare e certificale la sicurezza del sistema, individuare le vulnerabilità e suggerire mitigazioni alle vulnerabilità trovate, come macchina per effettuare il test è stata scelta un computer con O.S. **Kali Linux** per la suite di applicativi che offre.
Inoltre non è stato posto alcun vincolo sui danni possibili che possono conseguire dall'attività di testing.
Dato che la parte dell'asset di maggiore interesse è l'applicativo web hostato dalla stessa, la metodologia seguita è un framework generico composto dalle seguenti fasi:

1. Target Scoping
2. Information Gathering
3. Target Discovery
4. Enumerating Target
5. Vulnerabilty mapping
6. Target Exploitation
7. Post-Exploitation
8. Reporting

Vulnerability Report

Le vulnerabilità riscontrate durante le operazioni di penetration testing sono legate sia alla versione dei software utilizzati che alla loro implementazione.
Sfruttando tali vulnerabilità si può arrivare all'ottenimento di una shell di root.

Le vulnerabilità correlate alla versione dei sistemi software utilizzati possono portare alla violazione della disponibilità del servizio con attacchi di tipo DOS.
Tramite le implementazioni non sicure, come campi di testo non controllati e puliti in modo consono, si potranno effettuare degli attacchi di tipo XSS che sono molto comuni in questo ambito. Tali attacchi spesso hanno come obiettivo il controllo remoto della macchina e, tramite aumento di privilegi, l'ottenimento dei pieni poteri sulla macchina attaccata.

Vulnerabilità riscontrate:

1. Versione di Apache non aggiornata – Livello criticità: ALTO
    - 1.1. Apache/2.4.52 (Ubuntu)
    - 1.2. Questo tipo di criticità possono portare ad attacchi DOS da parte di utenti malevoli, in quanto ci sono vulnerabilità che possono essere sfruttate per compromettere la triade CIA.
2. Versione di OpenSSH non aggiornata – Livello criticità: ALTO
    - 2.1. OpenSSH 8.9p1
    - 2.2. Questo porta ad alcune vulnerabilità note come il seed scarso per i valori randomici, denial of service di alcuni servizi come ftpd, o addirittura authentication bypass su alcuni sistemi.
3. Campi di input non propriamente controllati – Livello criticità: ALTO
    - 3.1. Assenza di validazione e sanitizzazione dei campi di input che porta all'esecuzione di codice arbitrario sulla macchina target.
4. Credenziali database in chiaro, visibili nel codice sorgente – Livello criticità: ALTO
    - 4.1. Ottenendo il controllo da remoto della macchina target è possibile visualizzare il codice sorgente. Il problema principale, oltre alla possibilità di sfruttare vulnerabilità dovute alle funzioni nell'asset, è possibile visualizzare in chiaro le credenziali della base di dati che contiene dati sensibili sull'asset (in questo caso come fatture e utenti principalmente)
5. Possibilità di leggere certificati SSH di altri utenti – Livello criticità: ALTO
    - 5.1. Tramite un comando è possibile generare un file temporaneo che va a leggere il certificato dell'utente root per una connessione remota. Ciò permette di avere pieno accesso al sistema e tutto ciò che ne consegue.
6. Credenziali non opportunamente salvate del database – Livello criticità: MEDIO

6.1. All'interno del database gli utenti hanno solo l'hash con algoritmo SHA-256 e con la mancanza di eventuali salt.
6.2. L'utente usa le stesse credenziali pure per accedere localmente al sistema.

7. Possibilità di ottenere i cookie di sessione anche di utenti con permessi massimi – Livello criticità: MEDIO
   7.1. È possibile ottenere le credenziali di consuela anche tramite attacchi al dizionario in quanto semplice.
8. Il server divulga informazioni riguardo uptime e simili Livello criticità: BASSO
   8.1. Un attaccante potrebbe sfruttare queste conoscenze per sferrare attacchi.

Remediation Report

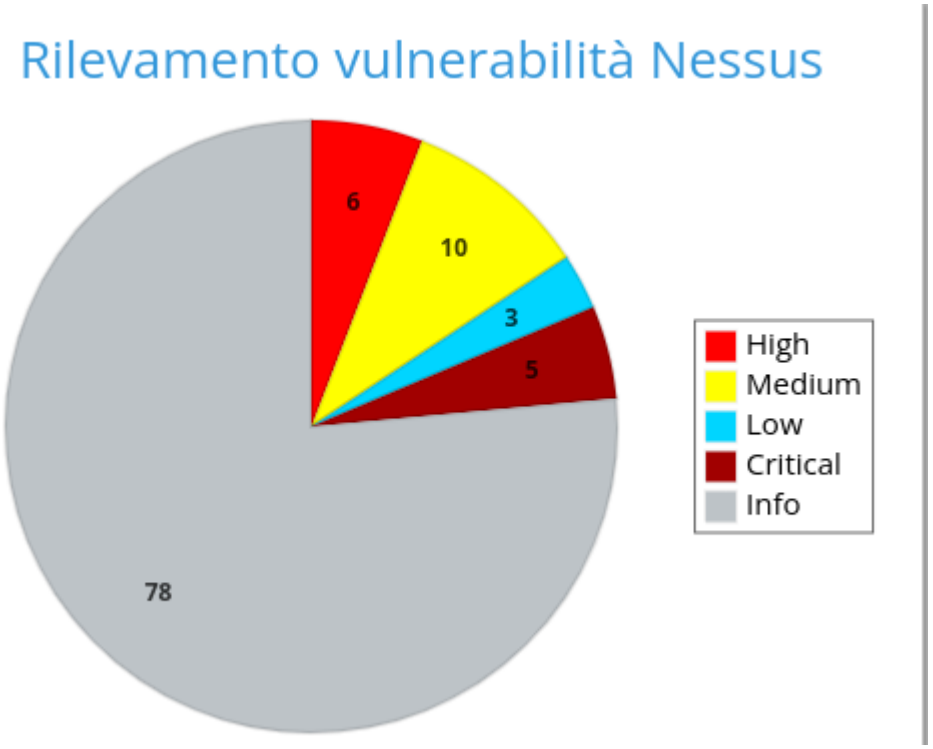
Il livello di sicurezza risultante dall'attività di penetration testing è risultato essere scadente. Tutte le vulnerabilità riscontrate devono essere rimediate ponendo particolare priorità alle vulnerabilità più gravi e che possono portare a seri danni del sistema, proseguendo poi con quelle con un livello di criticità più basso in modo decrescente. Esistono però rimediazioni alle criticità più gravi rilevate ed in questa parte del documento procediamo ad evidenziarle.

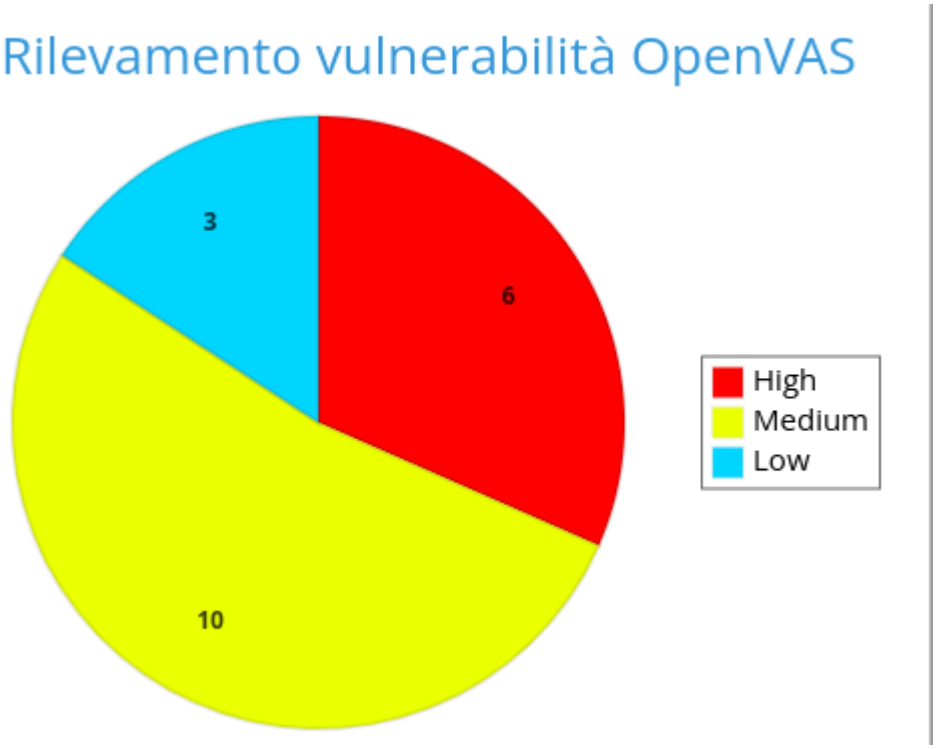
- Validare e sanificare i campi di input presenti all'interno della pagina che per aumentare il livello di safety.
- Aggiornare il sistema e i suoi componenti alle ultime versioni in modo da rimediare alle vulnerabilità dovute alle vecchie versioni del sistema.
- Rimuovere dati sensibili del sistema da punti facilmente accessibili dall'utente.
- Uso di password più robuste per gli utenti.
- Limitare i permessi di utenti non root.
- Pianificare Security Audits regolari per valutare e regolare il livello di scurezza del sistema, nonché la sua conformità agli standard.

Findings Summary

Le vulnerabilità sono suddivise su una scala con tre livelli di gravità:

1. High:
    1.1. Rischi critico per il sistema [CVSS ≥ 7.5]
2. Medim:
    2.1. Rischi elevato, vulnerabilità potenzialmente grave per il sistema [4≤CVSS<7.5]
3. Low:
    3.1. Rischi basso e vulnerabilità poco grave [CVSS<4]





Detailed Summary

HIGH

194474 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS. : less vulnerability (USN-6756-1)	**CVE** • CVE-2016-9840 [1] • CVE-2016-9841 [2] • CVE-2018-25032[3] • CVE-2022-37434[4]
High (CVSS: 9.8)	
Descrizione: L'host Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS. remoto ha installato un pacchetto che è affetto da una vulnerabilità, come indicato nell'advisory USN-6756-1. - less through 653 consente l'esecuzione di comandi del sistema operativo tramite un carattere newline nel nome di un file, perché il quoting è gestito in modo errato in filename.c. Lo sfruttamento richiede tipicamente l'uso di nomi di file controllati dall'aggressore, come i file estratti da un archivio non attendibile. L'exploit richiede anche la variabile d'ambiente LESSOPEN, ma questa è impostata per default inr molti casi comuni. (CVE-2024-32487)	
Impatto: Si è scoperto che zlib, venduto in klibc, gestiva in modo errato l'aritmetica dei puntatori. Un utente malintenzionato potrebbe sfruttare questo problema per causare il crash di klibc o per eseguire eventualmente codice arbitrario. (CVE-2016-9840, CVE-2016-9841) Danilo Ramos ha scoperto che zlib, venduto in klibc, gestiva in modo errato la memoria durante l'esecuzione di determinate operazioni di sgonfiaggio. Un utente	

malintenzionato potrebbe sfruttare questo problema per causare il crash di klibc o per eseguire eventualmente codice arbitrario. (CVE-2018-25032) Evgeny Legerov ha scoperto che zlib, venduto in klibc, gestiva in modo errato la memoria durante l'esecuzione di determinate operazioni di gonfiaggio. Un utente malintenzionato potrebbe sfruttare questo problema per causare il crash di klibc o per eseguire eventualmente codice arbitrario. (CVE-2022 37434)
Soluzione: VenditoreFix Installare i pacchetti aggiornati.
Metodo di detection: Vulnerabilità individuata con il tool OpenVas

198042 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Git vulnerabilities (USN-6793-1)	**CVE** • CVE-2024-32002[5] • CVE-2024-32004[6] • CVE-2024-32020[7] • CVE-2024-32021[8] • CVE-2024-32465[9]
High (CVSS: 9.0)	
Descrizione: Sull'host remoto Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS sono installati pacchetti che sono interessati da molteplici vulnerabilità, come indicato nell'avviso USN-6793-1. Si è scoperto che Git gestiva in modo errato alcuni sottomoduli. Un utente malintenzionato potrebbe sfruttare questo problema per eseguire codice arbitrario. Questo problema è stato risolto in Ubuntu 22.04 LTS, Ubuntu 23.10 e Ubuntu 24.04 LTS. (CVE-2024-32002) Si è scoperto che Git gestiva in modo errato alcuni repository clonati. Un utente malintenzionato potrebbe sfruttare questo problema per eseguire codice arbitrario. (CVE-2024-32004) È stato scoperto che Git gestiva in modo errato i cloni locali con file/directory collegati direttamente. Un utente malintenzionato potrebbe sfruttare questo problema per inserire un repository specializzato nel sistema locale del bersaglio. (CVE-2024-32020) Si è scoperto che Git gestiva in modo errato alcuni collegamenti simbolici. Un utente malintenzionato potrebbe sfruttare questo problema per influire sulla disponibilità e sull'integrità creando file arbitrari con collegamento fisico negli oggetti/nella directory del repository degli utenti. (CVE-2024-32021) Si è scoperto che Git gestiva in modo errato alcuni repository clonati. Un utente malintenzionato potrebbe sfruttare questo problema per eseguire codice arbitrario. (CVE-2024-32465) Tenable ha estratto il blocco di descrizione precedente direttamente dall'avviso sulla sicurezza di Ubuntu.	
Soluzione: VenditoreFix Installare i pacchetti aggiornati.	
Metodo di detection: Vulnerabilità individuata con il tool Nessus	

193362 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : klibc vulnerabilities (USN-6736-1)	**CVE** • CVE-2016-9840 [10] • CVE-2016-9841 [11] • CVE-2018-25032[12] • CVE-2022-37434[13]
High (CVSS: 9.0)	
Descrizione: L'host remoto Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 ha pacchetti installati che sono interessati da più vulnerabilità, come indicato nell'avviso USN-6736-1. - inftrees.c in zlib 1.2.8 potrebbe consentire agli aggressori dipendenti dal contesto di avere un impatto non specificato sfruttando l'aritmetica impropria dei puntatori. (CVE-2016-9840) - inffast.c in zlib 1.2.8 potrebbe consentire agli aggressori dipendenti dal contesto di avere un impatto non specificato sfruttando l'aritmetica impropria dei puntatori. (CVE-2016-9841) - zlib prima della versione 1.2.12 consente il danneggiamento della memoria durante lo sgonfiaggio (ovvero durante la compressione) se l'input ha molte corrispondenze distanti. (CVE-2018-25032) - zlib fino alla versione 1.2.12 ha un buffer over-read o buffer overflow basato su heap in inflate in inflate.c tramite un campo aggiuntivo di intestazione gzip di grandi dimensioni. NOTA: sono interessate solo le applicazioni che chiamano inflateGetHeader. Alcune applicazioni comuni raggruppano il codice sorgente zlib interessato ma potrebbero non essere in grado di chiamare inflateGetHeader (ad esempio, vedere il riferimento nodejs/node). (CVE-2022-37434)	
Soluzione: VenditoreFix Aggiorna i pacchetti klibc-utils, libklibc e/o libklibc-dev interessati.	
Metodo di detection: Vulnerabilità individuata con il tool Nessus	

198244 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GNU C Library vulnerabilities (USN-6804-1)	**CVE** • CVE-2024-33599[14] • CVE-2024-33600[15] • CVE-2024-33601[16] • CVE-2024-33602[17]
High (CVSS: 7.6)	
Descrizione: L'host remoto Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS ha pacchetti installati che sono interessati da più vulnerabilità, come indicato nell'avviso USN-6804-1. È stato scoperto che il demone nscd della libreria GNU C conteneva un buffer overflow basato su stack. Un utente malintenzionato locale potrebbe utilizzarlo per causare una negazione del servizio (arresto anomalo del sistema). (CVE-2024-33599) È stato scoperto che il demone nscd della libreria GNU C non controllava correttamente il contenuto della cache, causando una vulnerabilità di dereferenziazione del puntatore nullo. Un utente malintenzionato locale potrebbe utilizzarlo per causare una negazione del servizio (arresto anomalo del sistema). (CVE-2024-33600) È stato scoperto che il demone nscd della libreria GNU C non convalidava correttamente l'allocazione della memoria in determinate situazioni, portando a una	

vulnerabilità di dereferenziazione del puntatore nullo. Un utente malintenzionato locale potrebbe utilizzarlo per causare una negazione del servizio (arresto anomalo del sistema). (CVE-2024-33601)
È stato scoperto che il demone nscd della libreria GNU C non gestiva correttamente l'allocazione della memoria, il che potrebbe portare al danneggiamento della memoria. Un utente malintenzionato locale potrebbe utilizzarlo per causare una negazione del servizio (arresto anomalo del sistema).
(CVE-2024-33602)
Tenable ha estratto il blocco di descrizione precedente direttamente dall'avviso sulla sicurezza di Ubuntu.

Soluzione: VenditoreFix
Aggiorna i pacchetti klibc-utils, libklibc e/o libklibc-dev interessati.

Metodo di detection: Vulnerabilità individuata con il tool Nessus

192938 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : X.Org X Server vulnerabilities (USN-6721-1)	**CVE**
	• CVE-2024-31080[18] • CVE-2024-31081[19] • CVE-2024-31082[20] • CVE-2024-31083[21]

High (CVSS: 7.8)

Descrizione: L'host remoto Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 ha pacchetti installati che sono interessati da più vulnerabilità, come indicato nell'avviso USN-6721-1.
- È stata rilevata una vulnerabilità di sovralettura del buffer basata su heap nella funzione ProcXIGetSelectedEvents() del server X.org. Questo problema si verifica quando nelle risposte vengono utilizzati valori di lunghezza con scambio di byte, causando potenzialmente perdite di memoria ed errori di segmentazione, in particolare se attivati da un client con un endianness diverso. Questa vulnerabilità potrebbe essere sfruttata da un utente malintenzionato per far sì che il server X legga i valori della memoria heap e quindi li ritrasmetta al client finché non incontra una pagina non mappata, provocando un arresto anomalo. Nonostante l'incapacità dell'utente malintenzionato di controllare la memoria specifica copiata nelle risposte, i piccoli valori di lunghezza generalmente archiviati in un numero intero a 32 bit possono comportare significativi tentativi di lettura fuori dai limiti. (CVE-2024-31080)
- È stata rilevata una vulnerabilità di sovralettura del buffer basata su heap nella funzione ProcXIPassiveGrabDevice() del server X.org. Questo problema si verifica quando nelle risposte vengono utilizzati valori di lunghezza con scambio di byte, causando potenzialmente perdite di memoria ed errori di segmentazione, in particolare se attivati da un client con un endianness diverso. Questa vulnerabilità potrebbe essere sfruttata da un utente malintenzionato per far sì che il server X legga i valori della memoria heap e quindi li ritrasmetta al client finché non incontra una pagina non mappata, provocando un arresto anomalo. Nonostante l'incapacità dell'utente malintenzionato di controllare la memoria specifica copiata nelle risposte, i piccoli valori di lunghezza generalmente archiviati in un numero intero a

32 bit possono comportare significativi tentativi di lettura fuori dai limiti. (CVE-2024-31081) - È stata rilevata una vulnerabilità di sovralettura del buffer basata su heap nella funzione ProcAppleDRICreatePixmap() del server X.org. Questo problema si verifica quando nelle risposte vengono utilizzati valori di lunghezza con scambio di byte, causando potenzialmente perdite di memoria ed errori di segmentazione, in particolare se attivati da un client con un endianness diverso. Questa vulnerabilità potrebbe essere sfruttata da un utente malintenzionato per far sì che il server X legga i valori della memoria heap e quindi li ritrasmetta al client finché non incontra una pagina non mappata, provocando un arresto anomalo. Nonostante l'incapacità dell'utente malintenzionato di controllare la memoria specifica copiata nelle risposte, i piccoli valori di lunghezza generalmente archiviati in un numero intero a 32 bit possono comportare significativi tentativi di lettura fuori dai limiti. (CVE-2024-31082)
Soluzione: VenditoreFix Aggiorna i pacchetti klibc-utils, libklibc e/o libklibc-dev interessati.
Metodo di detection: Vulnerabilità individuata con il tool Nessus

198070 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GStreamer Base Plugins vulnerability (USN-6798-1)	**CVE** • CVE-2024-4453 [22]
High (CVSS: 7.8)	
Descrizione: Sull'host remoto Ubuntu 20.04 LTS/22.04 LTS/23.10/24.04 LTS sono installati pacchetti che sono interessati da una vulnerabilità, come indicato nell'avviso USN-6798-1. È stato scoperto che i plugin GStreamer Base gestivano in modo errato alcuni metadati EXIF. Un utente malintenzionato potrebbe sfruttare questo problema per eseguire codice arbitrario o causare un arresto anomalo del sistema. Tenable ha estratto il blocco di descrizione precedente direttamente dall'avviso sulla sicurezza di Ubuntu.	
Soluzione: VenditoreFix Aggiorna i pacchetti klibc-utils, libklibc e/o libklibc-dev interessati.	
Metodo di detection: Vulnerabilità individuata con il tool Nessus	

200099 - Ubuntu 22.04 LTS / 23.10 / 24.04 LTS : libarchive vulnerability (USN-6805-1)	**CVE** • CVE-2024-26256[23]
High (CVSS: 7.8)	
Descrizione: Sull'host remoto Ubuntu 22.04 LTS/23.10/24.04 LTS sono installati pacchetti che sono interessati da una vulnerabilità, come indicato nell'avviso USN-6805-1. È stato scoperto che libarchive gestiva in modo errato alcuni file di archivio RAR. Un utente malintenzionato potrebbe sfruttare questo problema per eseguire codice arbitrario o causare un arresto anomalo del sistema.	

Tenable ha estratto il blocco di descrizione precedente direttamente dall'avviso sulla sicurezza di Ubuntu.
Soluzione: VenditoreFix Aggiorna i pacchetti klibc-utils, libklibc e/o libklibc-dev interessati.
Metodo di detection: Vulnerabilità individuata con il tool Nessus

NVT: Ubuntu: Security Advisory (USN-6725-1)	**CVE**
	• CVE-2023-1194 [24] • CVE-2023-32254[25] • CVE-2023-32258[26] • CVE-2023-38427[27] • CVE-2023-38430[28] • CVE-2023-38431[29] • CVE-2023-3867 [30] • CVE-2023-46838[31] • CVE-2023-52340[32] • CVE-2023-52429[33] • CVE-2023-52436[34] • CVE-2023-52438[35] • CVE-2023-52439[36] • CVE-2023-52441[37] • CVE-2023-52442[38] • CVE-2023-52443[39] • CVE-2023-52444[40] • CVE-2023-52445[41] • CVE-2023-52448[42] • CVE-2023-52449[43] • CVE-2023-52451[44] • CVE-2023-52454[45] • CVE-2023-52456[46] • CVE-2023-52457[47] • CVE-2023-52458[48] • CVE-2023-52462[49] • CVE-2023-52463[50] • CVE-2023-52464[51] • CVE-2023-52467[52] • CVE-2023-52469[53] • CVE-2023-52470[54] • CVE-2023-52480[55] • CVE-2023-52609[56] • CVE-2023-52610[57] • CVE-2023-52612[58] • CVE-2024-22705[59] • CVE-2024-23850[60] • CVE-2024-23851[61] • CVE-2024-24860[62]

	• CVE-2024-26586[63] • CVE-2024-26589[64] • CVE-2024-26591[65] • CVE-2024-26597[66] • CVE-2024-26598[67] • CVE-2024-26631[68] • CVE-2024-26633[69]
High (CVSS: 9.8)	
Descrizione: Nell'host remoto manca un aggiornamento per "linux, linux-azure, linux-azure-5.15, linux-azure-fde, linux-azure-fde-5.15, linux-gcp, linux-gcp-5.15, linux-gke, linux-gkeop, linux-gkeop-5.15, linux-hwe-5.15, linux-ibm, linux-ibm-5.15, linux-intel-iotg, linux-intel-iotg-5.15, linux-kvm, linux-lowlatency, linux- pacchetti lowlatency-hwe-5.15, linux-nvidia, linux-oracle, linux-oracle-5.15, linux-raspi annunciati tramite l'avviso USN-6725-1.	
Impatto: Chih-Yen Chang ha scoperto che l'implementazione KSMBD nel kernel Linux non convalidava correttamente alcuni campi della struttura dati durante l'analisi dei contesti di lease, portando a una vulnerabilità di lettura fuori dai limiti. Un utente malintenzionato remoto potrebbe utilizzarlo per causare una negazione del servizio (arresto anomalo del sistema) o eventualmente esporre informazioni sensibili. (CVE-2023-1194) Quentin Minster ha scoperto che esisteva una condizione di competizione nell'implementazione KSMBD nel kernel Linux, che portava a una vulnerabilità use-after-free. Un utente malintenzionato remoto potrebbe utilizzarlo per causare un rifiuto di servizio (arresto anomalo del sistema) o eventualmente eseguire codice arbitrario. (CVE-2023-32254) È stato scoperto che esisteva una condizione di competizione nell'implementazione KSMBD nel kernel Linux durante la gestione delle connessioni di sessione, che portava a una vulnerabilità use-after-free. Un utente malintenzionato remoto potrebbe utilizzarlo per causare un rifiuto di servizio (arresto anomalo del sistema) o eventualmente eseguire codice arbitrario. (CVE-2023-32258) È stato scoperto che l'implementazione KSMBD nel kernel Linux non convalidava correttamente le dimensioni del buffer in determinate operazioni, causando un underflow degli interi e una vulnerabilità di lettura fuori dai limiti. Un utente malintenzionato remoto potrebbe utilizzarlo per causare una negazione del servizio (arresto anomalo del sistema) o eventualmente esporre informazioni sensibili. (CVE-2023-38427) Chih-Yen Chang ha scoperto che l'implementazione KSMBD nel kernel Linux non convalidava correttamente gli ID del protocollo di richiesta SMB, causando una vulnerabilità di lettura fuori dai limiti. Un utente malintenzionato remoto potrebbe utilizzarlo per causare un rifiuto di servizio (arresto anomalo del sistema). (CVE-2023-38430) Chih-Yen Chang ha scoperto che l'implementazione KSMBD nel kernel Linux non convalidava correttamente le dimensioni delle intestazioni dei pacchetti in determinate situazioni, portando a una vulnerabilità di lettura fuori dai limiti. Un utente malintenzionato remoto potrebbe utilizzarlo per causare una negazione del servizio (arresto anomalo del sistema) o eventualmente esporre informazioni sensibili. (CVE-2023 38431) È stato scoperto che l'implementazione KSMBD nel kernel Linux non gestiva correttamente le richieste di impostazione della sessione, causando una	

vulnerabilità di lettura fuori limite. Un utente malintenzionato remoto potrebbe utilizzarlo per esporre informazioni sensibili. (CVE-2023-3867)
Soluzione: VenditoreFix Installare i pacchetti aggiornati.
Metodo di detection: Vulnerabilità individuata con il tool OpenVas

NVT: Ubuntu: Security Advisory (USN-6766-1)	**CVE**
	• CVE-2023-52435[70] • CVE-2023-52486[71] • CVE-2023-52489[72] • CVE-2023-52491[73] • CVE-2023-52492[74] • CVE-2023-52493[75] • CVE-2023-52494[76] • CVE-2023-52498[77] • CVE-2023-52583[78] • CVE-2023-52587[79] • CVE-2023-52588[80] • CVE-2023-52594[81] • CVE-2023-52595[82] • CVE-2023-52597[83] • CVE-2023-52598[84] • CVE-2023-52599[85] • CVE-2023-52601[86] • CVE-2023-52602[87] • CVE-2023-52604[88] • CVE-2023-52606[89] • CVE-2023-52607[90] • CVE-2023-52608[91] • CVE-2023-52614[92] • CVE-2023-52615[93] • CVE-2023-52616[94] • CVE-2023-52617[95] • CVE-2023-52618[96] • CVE-2023-52619[97] • CVE-2023-52622[98] • CVE-2023-52623[99] • CVE-2023-52627[100] • CVE-2023-52631[101] • CVE-2023-52633[102] • CVE-2023-52635[103] • CVE-2023-52637[104] • CVE-2023-52638[105] • CVE-2023-52642[106] • CVE-2023-52643[107] • CVE-2024-1151 [108] • CVE-2024-2201 [109] • CVE-2024-23849[110]

	• CVE-2024-26592[111] • CVE-2024-26593[112] • CVE-2024-26594[113] • CVE-2024-26600[114] • CVE-2024-26602[115] • CVE-2024-26606[116] • CVE-2024-26608[117] • CVE-2024-26610[118] • CVE-2024-26614[119] • CVE-2024-26615[120] • CVE-2024-26625[121] • CVE-2024-26627[122] • CVE-2024-26635[123] • CVE-2024-26636[124] • CVE-2024-26640[125] • CVE-2024-26641[126] • CVE-2024-26644[127] • CVE-2024-26645[128] • CVE-2024-26660[129] • CVE-2024-26663[130] • CVE-2024-26664[131] • CVE-2024-26665[132] • CVE-2024-26668[133] • CVE-2024-26671[134] • CVE-2024-26673[135] • CVE-2024-26675[136] • CVE-2024-26676[137] • CVE-2024-26679[138] • CVE-2024-26684[139] • CVE-2024-26685[140] • CVE-2024-26689[141] • CVE-2024-26695[142] • CVE-2024-26696[143] • CVE-2024-26697[144] • CVE-2024-26698[145] • CVE-2024-26702[146] • CVE-2024-26704[147] • CVE-2024-26707[148] • CVE-2024-26712[149] • CVE-2024-26715[150] • CVE-2024-26717[151] • CVE-2024-26720[152] • CVE-2024-26722[153] • CVE-2024-26808[154] • CVE-2024-26825[155] • CVE-2024-26826[156] • CVE-2024-26829[157] • CVE-2024-26910[158] • CVE-2024-26916[159]

	• CVE-2024-26920[160]
High (CVSS: 7.8)	
Descrizione: Nell'host remoto manca un aggiornamento per "linux, linux-azure, linux-azure-5.15, linux-azure-fde, linux-azure-fde-5.15, linux-gcp, linux-gcp-5.15, linux-gke, linux-gkeop, linux-gkeop-5.15, linux-ibm, linux-ibm-5.15, linux-kvm, linux-lowlatency, linux-lowlatency-hwe-5.15, linux-nvidia, linux-oracle, linux-oracle-5.15' pacchetto(i) annunciato tramite l'avviso USN-6766-1.	
Impatto: È stato scoperto che l'implementazione Open vSwitch nel kernel Linux potrebbe traboccare il suo stack durante operazioni di azioni ricorsive in determinate condizioni. Un utente malintenzionato locale potrebbe utilizzarlo per causare una negazione del servizio (arresto anomalo del sistema). (CVE-2024-1151) Sander Wiebing, Alvise de Faveri Tron, Herbert Bos e Cristiano Giuffrida hanno scoperto che le mitigazioni del kernel Linux per la vulnerabilità iniziale Branch History Injection (CVE-2022-0001) erano insufficienti per i processori Intel. Un utente malintenzionato locale potrebbe potenzialmente utilizzarlo per esporre informazioni sensibili. (CVE-2024-2201) Chenyuan Yang ha scoperto che l'implementazione del protocollo RDS nel kernel Linux conteneva una vulnerabilità di lettura fuori dai limiti. Un utente malintenzionato potrebbe utilizzarlo per causare un rifiuto del servizio (arresto anomalo del sistema). (CVE-2024-23849)	
Soluzione: VenditoreFix Installare i pacchetti aggiornati.	
Metodo di detection: Vulnerabilità individuata con il tool OpenVas	

NVT: Ubuntu: Security Advisory (USN-6742-1)	**CVE**
	• CVE-2023-24023[161] • CVE-2023-52600[162] • CVE-2023-52603[163] • CVE-2024-26581[164]
High (CVSS: 7.8)	
Descrizione: Nell'host remoto manca un aggiornamento per "linux, linux-aws, linux-aws-5.15, linux-azure-5.15, linux-azure-fde, linux-azure-fde-5.15, linux-gcp, linux-gcp- 5.15, linux-gke, linux-gkeop, linux-gkeop-5.15, linux-hwe-5.15, linux-ibm, linux-ibm-5.15, linux-intel-iotg, linux-intel-iotg-5.15, linux-kvm, pacchetto/i linux-lowlatency-hwe-5.15, linux-oracle, linux-oracle-5.15, linux-raspi' annunciati tramite l'avviso USN-6742-1.	
Impatto: Daniele Antonioli ha scoperto che l'accoppiamento Secure Simple Pairing e Secure Connections nel protocollo Bluetooth potrebbe consentire a un utente non autenticato di completare l'autenticazione senza accoppiare le credenziali. Un utente malintenzionato fisicamente vicino posto tra due dispositivi Bluetooth potrebbe utilizzarlo per impersonare successivamente uno dei dispositivi accoppiati. (CVE-2023-24023) Sono stati scoperti diversi problemi di sicurezza nel kernel Linux. Un utente malintenzionato potrebbe utilizzarli per compromettere il sistema. Questo aggiornamento corregge aws nei seguenti sottosistemi: - le system JFS, - Net lter, (CVE-2024-26581, CVE-2023-52600, CVE-2023-52603)	

Soluzione: VenditoreFix Installare i pacchetti aggiornati.
Metodo di detection: Vulnerabilità individuata con il tool OpenVas

NVT: Ubuntu: Security Advisory (USN-6735-1)	**CVE**
	• CVE-2023-30588[165] • CVE-2023-30589[166] • CVE-2023-30590[167]
High (CVSS: 7.5)	
Descrizione: All'host remoto manca un aggiornamento per i pacchetti "node js" annunciati tramite l'avviso USN-6735-1.	
Impatto: È stato scoperto che Node.js gestiva in modo errato l'uso di chiavi pubbliche non valide durante la creazione di un certificato x509. Se un utente o un sistema automatizzato venisse indotto con l'inganno ad aprire un file di input appositamente predisposto, un utente malintenzionato remoto potrebbe sfruttare questo problema per causare una negazione del servizio. Questo problema riguardava solo Ubuntu 23.10. (CVE-2023-30588) Si è scoperto che Node.js gestiva erroneamente l'uso delle sequenze CRLF per delimitare le richieste HTTP. Se un utente o un sistema automatizzato venisse indotto con l'inganno ad aprire un le di input appositamente predisposto, un utente malintenzionato remoto potrebbe sfruttare questo problema per ottenere un accesso non autorizzato. Questo problema riguardava solo Ubuntu 23.10. (CVE-2023-30589) È stato scoperto che Node.js descriveva erroneamente la funzione generateKeys() nella documentazione. Questa incoerenza potrebbe portare a problemi di sicurezza nelle applicazioni che utilizzano queste API. (CVE-2023-30590)	
Soluzione: VenditoreFix Installare i pacchetti aggiornati.	
Metodo di detection: Vulnerabilità individuata con il tool OpenVas	

NVT: Ubuntu: Security Advisory (USN-6754-1)	**CVE**
	• CVE-2019-9511 [168] • CVE-2019-9513 [169] • CVE-2023-44487[170] • CVE-2024-28182[171]
High (CVSS: 7.5)	
Descrizione: All'host remoto manca un aggiornamento per i pacchetti "nghttp2" annunciati tramite l'avviso USN-6754-1.	
Impatto: È stato scoperto che nghttp2 gestiva in modo errato l'implementazione HTTP/2. Un utente malintenzionato remoto potrebbe sfruttare questo problema per far sì che nghttp2 consumi risorse, portando a una negazione del servizio. Questo problema riguardava solo Ubuntu 16.04 LTS e Ubuntu 18.04 LTS. (CVE-2019-9511, CVE-2019-9513)	

È stato scoperto che nghttp2 gestiva in modo errato l'annullamento delle richieste. Un utente malintenzionato remoto potrebbe sfruttare questo problema per far sì che nghttp2 consumi risorse, portando a una negazione del servizio. Questo problema riguardava solo Ubuntu 16.04 LTS e Ubuntu 18.04 LTS. (CVE-2023-44487) Si è scoperto che nghttp2 potrebbe essere in grado di elaborare un numero illimitato di frame CONTINUATION HTTP/2. Un utente malintenzionato remoto potrebbe sfruttare questo problema per far sì che nghttp2 consumi risorse, portando a una negazione del servizio. (CVE-2024-28182)
Soluzione: VenditoreFix Installare i pacchetti aggiornati.
Metodo di detection: Vulnerabilità individuata con il tool OpenVas

MEDIUM

NVT: Ubuntu: Security Advisory (USN-6727-1)	**CVE**
	• CVE-2023-4421 [172] • CVE-2023-5388 [173] • CVE-2023-6135 [174]
Medium (CVSS: 6.5)	
Descrizione: All'host remoto manca un aggiornamento per i pacchetti 'nss' annunciati tramite l'avviso USN-6727-1.	
Impatto: È stato scoperto che NSS gestiva in modo errato il riempimento durante il controllo dei certificati PKCS#1. Un utente malintenzionato remoto potrebbe sfruttare questo problema per eseguire attacchi simili a Bleichenbacher e recuperare dati privati. Questo problema riguardava solo Ubuntu 20.04 LTS. (CVE-2023-4421) Si è scoperto che NSS aveva un canale laterale temporale durante l'esecuzione della decrittazione RSA. Un utente malintenzionato remoto potrebbe sfruttare questo problema per recuperare dati privati. (CVE-2023-5388) Si è scoperto che NSS aveva un canale laterale di temporizzazione quando si utilizzavano determinate curve NIST. Un utente malintenzionato remoto potrebbe sfruttare questo problema per recuperare dati privati. (CVE-2023-6135) Il pacchetto NSS conteneva certificati CA obsoleti. Questo aggiornamento aggiorna il pacchetto NSS alla versione 3.98 che include l'ultimo bundle di certificati CA e altri miglioramenti della sicurezza.	
Soluzione: VenditoreFix Installare i pacchetti aggiornati.	
Metodo di detection: Vulnerabilità individuata con il tool OpenVas	

136929 - JQuery 1.2 < 3.5.0 Multiple XSS	**CVE**
	• CVE-2020-11022[175] • CVE-2020-11023[176]

Medium (CVSS: 6.1)
Descrizione: Secondo la versione auto-riportata nello script, la versione di JQuery ospitata sul server Web remoto è maggiore o uguale a 1.2 e precedente a 3.5.0. È quindi affetto da molteplici vulnerabilità di cross site scripting. Tieni presente che le vulnerabilità a cui si fa riferimento in questo plug-in non hanno alcun impatto sulla sicurezza su PAN-OS e/o gli scenari richiesti per uno sfruttamento efficace non esistono sui dispositivi che eseguono una versione PAN-OS.
Soluzione: VenditoreFix Aggiorna a JQuery versione 3.5.0 o successiva.
Metodo di detection: Vulnerabilità individuata con il tool Nessus

NVT: Ubuntu: Security Advisory (USN-6727-2)	**CVE**
	• CVE-2023-4421 [177] • CVE-2023-5388 [178] • CVE-2023-6135 [179]
Medium (CVSS: 6.5)	
Descrizione: All'host remoto manca un aggiornamento per i pacchetti 'nss' annunciati tramite l'avviso USN-6727-2.	
Impatto: USN-6727-1 ha risolto le vulnerabilità in NSS. L'aggiornamento ha introdotto una regressione durante il tentativo di caricare moduli di sicurezza su Ubuntu 20.04 LTS e Ubuntu 22.04 LTS. Questo aggiornamento risolve il problema. Ci scusiamo per il disagio. Dettagli dell'avviso originale: è stato scoperto che NSS gestiva in modo errato il riempimento durante il controllo dei certificati PKCS#1. Un utente malintenzionato remoto potrebbe sfruttare questo problema per eseguire attacchi simili a Bleichenbacher e recuperare dati privati. Questo problema riguardava solo Ubuntu 20.04 LTS. (CVE-2023-4421) Si è scoperto che NSS aveva un canale laterale temporale durante l'esecuzione della decrittazione RSA. Un utente malintenzionato remoto potrebbe sfruttare questo problema per recuperare dati privati. (CVE-2023-5388) Si è scoperto che NSS aveva un canale laterale di temporizzazione quando si utilizzavano determinate curve NIST. Un utente malintenzionato remoto potrebbe sfruttare questo problema per recuperare dati privati. (CVE-2023-6135) Il pacchetto NSS conteneva certificati CA obsoleti. Questo aggiornamento aggiorna il pacchetto NSS alla versione 3.98 che include l'ultimo bundle di certificati CA e altri miglioramenti della sicurezza.	
Soluzione: VenditoreFix Installare i pacchetti aggiornati.	
Metodo di detection: Vulnerabilità individuata con il tool OpenVas	

NVT: Ubuntu: Security Advisory (USN-6719-2)	**CVE**
	• CVE-2024-28085[180]
Medium (CVSS: 5.0)	
Descrizione: All'host remoto manca un aggiornamento per i pacchetti 'util-linux' annunciati tramite l'avviso USN-6719-2.	
Impatto: USN-6719-1 ha risolto una vulnerabilità in util-linux. Sfortunatamente, si è scoperto che la correzione non risolveva completamente il problema. Questo aggiornamento rimuove il bit di autorizzazione setgid dal muro e scrive le utilità. Dettagli dell'avviso originale: Skyler Ferrante ha scoperto che il comando wall util-linux non filtrava le sequenze di escape dagli argomenti della riga di comando. Un utente malintenzionato locale potrebbe sfruttare questo problema per ottenere informazioni riservate.	
Soluzione: VenditoreFix Installare i pacchetti aggiornati.	
Metodo di detection: Vulnerabilità individuata con il tool OpenVas	

NVT: Ubuntu: Security Advisory (USN-6729-1)	**CVE**
	• CVE-2023-38709[181] • CVE-2024-24795[182] • CVE-2024-27316[183]
Medium (CVSS: 5.0)	
Descrizione: All'host remoto manca un aggiornamento per i pacchetti "apache2" annunciati tramite l'avviso USN-6729-1.	
Impatto: Orange Tsai ha scoperto che il server HTTP Apache gestiva in modo errato la convalida di determinati input. Un utente malintenzionato remoto potrebbe sfruttare questo problema per eseguire attacchi di suddivisione delle richieste HTTP. (CVE-2023-38709) Keran Mu e Jianjun Chen hanno scoperto che il server HTTP Apache veniva gestito in modo errato convalidare determinati input. Un utente malintenzionato remoto potrebbe sfruttare questo problema per eseguire attacchi di suddivisione delle richieste HTTP. (CVE-2024-24795) Bartek Nowotarski ha scoperto che il modulo Apache HTTP Server HTTP/2 gestiva in modo errato i frame di continuazione infiniti. Un utente malintenzionato remoto potrebbe sfruttare questo problema per far sì che il server consumi risorse, determinando una negazione del servizio. (CVE-2024-27316)	
Soluzione: VenditoreFix Installare i pacchetti aggiornati.	
Metodo di detection: Vulnerabilità individuata con il tool OpenVas	

	CVE

NVT: Ubuntu: Security Advisory (USN-6755-1)	• CVE-2023-7207 [184]
Medium (CVSS: 5.0)	
Descrizione: All'host remoto manca un aggiornamento per i pacchetti 'cpio' annunciati tramite l'avviso USN-6755-1.	
Impatto: Ingo Bruckl ha scoperto che cpio conteneva una vulnerabilità di tipo path traversal. Se un utente o un sistema automatizzato venisse indotto con l'inganno a estrarre un archivio cpio appositamente predisposto, un utente malintenzionato potrebbe sfruttare questo problema per scrivere file arbitrari all'esterno della directory di destinazione sull'host, anche se utilizza l'opzione no-absolute-filenames.	
Soluzione: VenditoreFix Installare i pacchetti aggiornati.	
Metodo di detection: Vulnerabilità individuata con il tool OpenVas	

NVT: Ubuntu: Security Advisory (USN-6756-1)	**CVE**
	• CVE-2024-32487[185]
Medium (CVSS: 5.0)	
Descrizione: All'host remoto manca un aggiornamento per i pacchetti "meno" annunciati tramite l'avviso USN-6756-1.	
Impatto: Si è scoperto che i caratteri di nuova riga nei nomi dei file venivano gestiti in modo meno errato. Se un utente o un sistema automatizzato venisse indotto con l'inganno ad aprire file appositamente predisposti, un utente malintenzionato potrebbe sfruttare questo problema per eseguire comandi arbitrari sull'host.	
Soluzione: VenditoreFix Installare i pacchetti aggiornati.	
Metodo di detection: Vulnerabilità individuata con il tool OpenVas	

NVT: Ubuntu: Security Advisory (USN-6737-1)	**CVE**
	• CVE-2024-2961[186]
Medium (CVSS: 5.0)	
Descrizione: All'host remoto manca un aggiornamento per i pacchetti 'glibc' annunciati tramite l'avviso USN-6737-1.	
Impatto: Charles Fol ha scoperto che la funzionalità iconv della libreria GNU C gestiva in modo errato alcune sequenze di input. Un utente malintenzionato potrebbe sfruttare questo problema per causare l'arresto anomalo della libreria GNU C, con conseguente negazione del servizio o eventualmente eseguire codice arbitrario.	
Soluzione: VenditoreFix Installare i pacchetti aggiornati.	
Metodo di detection: Vulnerabilità individuata con il tool OpenVas	

NVT: Ubuntu: Security Advisory (USN-6768-1)	**CVE**
	• CVE-2024-34397[187]
Medium (CVSS: 5.0)	
Descrizione: All'host remoto manca un aggiornamento per i pacchetti "glib2.0" annunciati tramite l'avviso USN-6768-1.	
Impatto: Alicia Boya Garcia ha scoperto che GLib gestiva in modo errato gli abbonamenti ai segnali. Un utente malintenzionato locale potrebbe sfruttare questo problema per falsificare i segnali D-Bus provocando una serie di impatti tra cui una possibile escalation dei privilegi.	
Soluzione: VenditoreFix Installare i pacchetti aggiornati.	
Metodo di detection: Vulnerabilità individuata con il tool OpenVas	

NVT: Ubuntu: Security Advisory (USN-6733-1)	**CVE**
	• CVE-2024-28834[188] • CVE-2024-28835[189]
Medium (CVSS: 5.0)	
Descrizione: All'host remoto manca un aggiornamento per i pacchetti "gnutls28" annunciati tramite l'avviso USN-6733-1.	
Impatto: Si è scoperto che GnuTLS aveva un canale laterale temporale durante l'esecuzione di determinate operazioni ECDSA. Un utente malintenzionato remoto potrebbe sfruttare questo problema per recuperare informazioni riservate. (CVE-2024-28834) È stato scoperto che GnuTLS gestiva in modo errato la verifica di alcuni bundle PEM. Un utente malintenzionato remoto potrebbe sfruttare questo problema per causare l'arresto anomalo di GnuTLS, con conseguente negazione del servizio. Questo problema riguardava solo Ubuntu 22.04 LTS e Ubuntu 23.10. (CVE-2024-28835)	
Soluzione: VenditoreFix Installare i pacchetti aggiornati.	
Metodo di detection: Vulnerabilità individuata con il tool OpenVas	

NVT: Cleartext Transmission of Sensitive Information via HTTP	**CVE**
	• https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
Medium (CVSS: 4.8)	

Descrizione: L'host/applicazione trasmette informazioni sensibili (nome utente, password) in chiaro tramite HTTP.
Impatto: Un utente malintenzionato potrebbe sfruttare questa situazione per compromettere o intercettare la comunicazione HTTP tra il client e il server utilizzando un attacco man-in-the-middle per ottenere l'accesso a dati sensibili come nomi utente o password.
Soluzione: Soluzione alternativa Imponi la trasmissione di dati sensibili tramite una connessione SSL/TLS crittografata. Assicurati inoltre che l'host/l'applicazione reindirizzi tutti gli utenti alla connessione SSL/TLS protetta prima di consentire l'inserimento di dati sensibili nelle funzioni menzionate
Metodo di detection: Vulnerabilità individuata con il tool OpenVas

198044 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Jinja2 vulnerability (USN-6787-1)	**CVE** • CVE-2024-34064[190]
Medium (CVSS: 5.4)	
Descrizione: L'host remoto Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS ha pacchetti installati che sono interessati da una vulnerabilità come indicato nell'avviso USN-6787-1. Si è scoperto che Jinja2 gestiva in modo errato alcuni attributi HTML accettati dal filtro xmlattr. Un utente malintenzionato potrebbe sfruttare questo problema per inserire chiavi e valori di attributi HTML arbitrari per eseguire potenzialmente un attacco XSS (cross-site scripting). Tenable ha estratto il blocco di descrizione precedente direttamente dall'avviso sulla sicurezza di Ubuntu.	
Soluzione: VenditoreFix Aggiorna i pacchetti python-jinja2 e/o python3-jinja2 interessati.	
Metodo di detection: Vulnerabilità individuata con il tool Nessus	

197569 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : idna vulnerability (USN-6780-1)	**CVE** • CVE-2024-3651 [191]
Medium (CVSS: 6.5)	
Descrizione: L'host remoto Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS ha pacchetti installati che sono interessati da una vulnerabilità come indicato nell'avviso USN-6780-1. Guido Vranken ha scoperto che idna non gestiva correttamente alcuni input, che potrebbe comportare un consumo significativo di risorse. Un aggressore potrebbe possibilmente utilizzare questo problema per causare una negazione del servizio.	
Soluzione: VenditoreFix	

Aggiorna i pacchetti pypy-idna, python-idna e/o python3-idna interessati.
Metodo di detection: Vulnerabilità individuata con il tool Nessus

198063 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : TPM2 Software Stack vulnerabilities (USN-6796-1)	**CVE**
	• CVE-2023-22745[192] • CVE-2024-29040[193]
Medium (CVSS: 6.4)	
Descrizione: Sull'host remoto Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS sono installati pacchetti che sono interessati da molteplici vulnerabilità, come indicato nell'avviso USN-6796-1. Fergus Dall ha scoperto che lo stack software TPM2 non gestiva correttamente gli array di livelli. Un utente malintenzionato potrebbe sfruttare questo problema per causare l'arresto anomalo dello stack software TPM2, con conseguente negazione del servizio, o eventualmente eseguire codice arbitrario. (CVE-2023-22745) Jurgen Repp e Andreas Fuchs hanno scoperto che TPM2 Software Stack non convalidava i dati del preventivo dopo la deserializzazione. Un utente malintenzionato potrebbe generare una citazione arbitraria e causare un comportamento sconosciuto dello stack software TPM2. (CVE-2024-29040)	
Soluzione: VenditoreFix Aggiorna i pacchetti interessati.	
Metodo di detection: Vulnerabilità individuata con il tool Nessus	

197214 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6775-1)	**CVE**
	• CVE-2023-47233[194] • CVE-2023-52530[195] • CVE-2024-26622[196]
Medium (CVSS: 4.3)	
Descrizione: Sull'host remoto Ubuntu 20.04 LTS/22.04 LTS è installato un pacchetto affetto da molteplici vulnerabilità, come indicato nell'avviso USN-6775-1. - Il componente brcm80211 nel kernel Linux fino alla versione 6.5.10 ha un codice brcmf_cfg80211_detach use-after-free nel codice di disconnessione del dispositivo (disconnessione dell'USB tramite hotplug). Per gli aggressori fisicamente vicini con accesso locale, questo potrebbe essere sfruttato in uno scenario reale. Questo è correlato a brcmf_cfg80211_escan_timeout_worker in drivers/net/wireless/broadcom/brcm80211/brcmfmac/cfg80211.c. (CVE-2023-47233) - Nel kernel Linux, la seguente vulnerabilità è stata risolta: wifi: mac80211: corretto il potenziale utilizzo della chiave - after-free Quando ieee80211_key_link() viene chiamato da ieee80211_gtk_rekey_add() ma restituisce o a causa della protezione KRACK (reinstallazione della chiave identica), ieee80211_gtk_rekey_add( ) restituirà comunque un puntatore alla chiave, in un potenziale use-after-free. Questo	

normalmente non accade poiché viene chiamato da iwlwifi solo in caso di offload di rekey WoWLAN che ha la propria protezione KRACK, ma è comunque meglio risolverlo, farlo restituendo un codice di errore e convertendolo in successo solo sul limite cfg80211, lasciando l'errore per i chiamanti errati di ieee80211_gtk_rekey_add(). (CVE-2023-52530) - Nel kernel Linux, la seguente vulnerabilità è stata risolta: tomoyo: corretto il bug di scrittura UAF in tomoyo_write_control() Poiché tomoyo_write_control() aggiorna head->write_buf quando viene richiesta write() di righe lunghe, dobbiamo recuperare head->write_buf dopo che head->io_sem viene mantenuto. In caso contrario, le richieste write() simultanee possono causare problemi di use-after-free-write e double-free. (CVE-2024-26622)
Soluzione: VenditoreFix Aggiorna i pacchetti del kernel interessati.
Metodo di detection: Vulnerabilità individuata con il tool Nessus

LOW

NVT: ICMP Timestamp Reply Information Disclosure	**CVE**
	• CVE-1999-0524 [197]
Low (CVSS: 2.1)	
Descrizione: L'host remoto ha risposto a una richiesta di timestamp ICMP.	
Impatto: Queste informazioni potrebbero teoricamente essere utilizzate per sfruttare generatori di numeri casuali deboli basati sul tempo in altri servizi.	
Soluzione: Mitigazione Sono possibili diverse attenuazioni: • Disabilitare completamente il supporto per il timestamp ICMP sull'host remoto • Proteggi l'host remoto tramite un rewall e blocca i pacchetti ICMP che passano attraverso il firewall in entrambe le direzioni (completamente o solo per reti non attendibili)	
Metodo di detection: Vulnerabilità individuata con il tool OpenVas	

NVT: TCP Timestamps Information Disclosure	**CVE**
	• https://datatracker.ietf.org/doc/html/rfc1323
Low (CVSS: 2.1)	
Descrizione: L'host remoto implementa i timestamp TCP e quindi consente di calcolare il tempo di attività.	

Impatto: Un effetto collaterale di questa funzionalità è che a volte è possibile calcolare il tempo di attività dell'host remoto.
Soluzione: Mitigazione Per disabilitare i timestamp TCP su Linux aggiungere la riga 'net.ipv4.tcp_timestamps = 0' a /etc/sysctl.conf. Eseguire 'sysctl -p' per applicare le impostazioni in fase di runtime. Per disabilitare i timestamp TCP su Windows eseguire 'netsh int tcp set global timestamps=disabled' A partire da Windows Server 2008 e Vista, il timestamp non può essere completamente disabilitato. Il comportamento predefinito dello stack TCP/IP su questo sistema consiste nel non utilizzare le opzioni Timestamp quando si avviano le connessioni TCP, ma utilizzarle se il peer TCP che sta avviando la comunicazione le include nel proprio segmento di sincronizzazione (SYN).
Metodo di detection: Vulnerabilità individuata con il tool OpenVas

NVT: Weak MAC Algorithm(s) Supported (SSH)	**CVE**
	• CVE-1999-0524 [198]
Low (CVSS: 2.6)	
Descrizione: Il server SSH remoto è configurato per consentire/supportare algoritmi MAC deboli.	
Soluzione: Mitigazione Disabilitare gli algoritmi MAC deboli segnalati.	
Metodo di detection: Vulnerabilità individuata con il tool OpenVas	

ALTRE

Debole rispetto ad attacchi XSS	**CVE**
High	
Descrizione: Il server accetta payload contenenti codie JS malevolo che possono portare all'esecuzione arbitraria di codice	
Soluzione: Sanificare i campi di input	
Metodo di detection: Vulnerabilità individuata a mano	

Flask	**CVE**
	• -
Low	

Descrizione: Il server contiene delle credenziali di accesso al database che non dovrebbero essere visibili all'esterno.
Soluzione: Salvare i dati in accessibili da utenti non root.
Metodo di detection: Vulnerabilità individuata a mano

qpdf	**CVE**
	• -
High	
Descrizione: Possibile data leakage di informazioni sensibili come chiavi RSA per il servizio OpenSSH di utenti root.	
Soluzione: Limitare l'esecuzione di programmi a utenti privilegiati.	
Metodo di detection: Vulnerabilità individuata a mano	

mysql	**CVE**
	• -
Medium	
Descrizione: Debole sicurezza nel salvataggio delle password in quanto non è presente alcun salt, le password vengono solo hashate con algoritmo HASH-256.	
Soluzione: Implementare tecniche di offuscamento migliori.	
Metodo di detection: Vulnerabilità individuata a mano	

Credenziali	**CVE**
	• -
Low	
Descrizione: Gli utenti del sistema utilizzano le stesse credenziali sia per accedere alla Web App che alla macchina locale.	
Soluzione: Implementare tecniche di offuscamento migliori.	
Metodo di detection: Vulnerabilità individuata a mano	

Credenziali deboli	**CVE**
	• -
Low	
Descrizione: Alcuni utenti presentano password facilmente riottenibili tramite password cracking.	
Soluzione: Utilizzare password più robuste	
Metodo di detection: Vulnerabilità individuata a mano	

Appendix

Tali vulnerabilità sono tutte sfruttabili come dimostrato e illustrato passo per passo all'interno del documento di **Penetration Testing Narrative**.

References

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9840
[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9841
[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-25032
[4] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37434
[5] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-32002
[6] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-32004
[7] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-32020
[8] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-32021
[9] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-32465
[10] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9840
[11] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9841
[12] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-25032
[13] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37434
[14] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-33599
[15] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-33600
[16] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-33601
[17] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-33602
[18] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-31080
[19] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-31081
[20] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-31082
[21] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-31083
[22] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-4453
[23] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26256
[24] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-1194
[25] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-32254
[26] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-32258
[27] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38427
[28] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38430
[29] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38431
[30] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-3867
[31] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-46838
[32] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52340
[33] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52429
[34] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52436
[35] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52438
[36] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52439
[37] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52441
[38] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52442
[39] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52443
[40] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52444
[41] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52445
[42] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52448
[43] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52449
[44] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52451
[45] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52454

[46] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52456
[47] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52457
[48] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52458
[49] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52462
[50] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52463
[51] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52464
[52] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52467
[53] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52469
[54] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52470
[55] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52480
[56] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52609
[57] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52610
[58] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52612
[59] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-22705
[60] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23850
[61] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23851
[62] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24860
[63] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26586
[64] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26589
[65] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26591
[66] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26597
[67] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26598
[68] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26631
[69] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26633
[70] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52435
[71] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52486
[72] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52489
[73] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52491
[74] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52492
[75] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52493
[76] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52494
[77] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52498
[78] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52583
[79] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52587
[80] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52588
[81] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52594
[82] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52595
[83] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52597
[84] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52598
[85] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52599
[86] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52601
[87] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52602
[88] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52604
[89] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52606
[90] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52607
[91] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52608
[92] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52614

[93] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52615
[94] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52616
[95] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52617
[96] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52618
[97] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52619
[98] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52622
[99] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52623
[100] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52627
[101] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52631
[102] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52633
[103] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52635
[104] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52637
[105] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52638
[106] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52642
[107] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52643
[108] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-1151
[109] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-2201
[110] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23849
[111] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26592
[112] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26593
[113] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26594
[114] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26600
[115] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26602
[116] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26606
[117] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26608
[118] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26610
[119] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26614
[120] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26615
[121] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26625
[122] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26627
[123] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26635
[124] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26636
[125] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26640
[126] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26641
[127] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26644
[128] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26645
[129] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26660
[130] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26663
[131] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26664
[132] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26665
[133] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26668
[134] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26671
[135] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26673
[136] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26675
[137] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26676
[138] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26679
[139] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26684

[140] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26685
[141] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26689
[142] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26695
[143] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26696
[144] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26697
[145] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26698
[146] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26702
[147] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26704
[148] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26707
[149] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26712
[150] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26715
[151] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26717
[152] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26720
[153] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26722
[154] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26808
[155] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26825
[156] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26826
[157] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26829
[158] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26910
[159] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26916
[160] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26920
[161] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24023
[162] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52600
[163] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52603
[164] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26581
[165] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-30588
[166] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-30589
[167] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-30590
[168] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9511
[169] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9513
[170] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44487
[171] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-28182
[172] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4421
[173] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5388
[174] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-6135
[175] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11022
[176] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11023
[177] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4421
[178] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5388
[179] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-6135
[180] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-28085
[181] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38709
[182] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24795
[183] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-27316
[184] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-7207
[185] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-32487
[186] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-2961

[187] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-34397
[188] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-28834
[189] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-28835
[190] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-34064
[191] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-3651
[192] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22745
[193] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-29040
[194] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-47233
[195] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-52530
[196] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26622
[197] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0524
[198] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0524