# W12D1 - Pratica 1

Giacomo di Giacinto


**Traccia:**

Effettuare un Vulnerability Assessment con Nessus sulla macchina **Metasploitable** indicando come target **solo** le **porte comuni** (potete scegliere come scansione il «basic network scan», o l'advanced e poi configurarlo)

A valle del completamento della scansione, **analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web**.

Gli obiettivi dell'esercizio sono:

- **Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni**
- **Familiarizzare con alcune delle vulnerabilità note che troverete spesso sul vostro percorso da penetration tester**

**Consegna:**

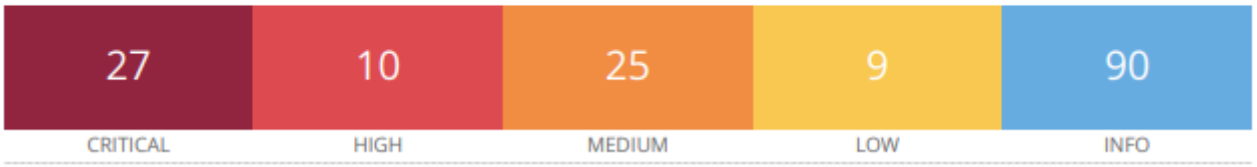
- Report PDF per «tecnico»

Report tecnico è inteso come "quasi completo" che va ad indicare sia le porte che la vulnerabilità che la risoluzione, in modo da poter intervenire.

- Suggerimento: fare traduzione in italiano della descrizione e/o remediation

Attraverso il software Nessus eseguo il vulnerability assestment sulla macchina Metasploitable e, di seguito incollo il risultato.

## 192.168.1.246




Vulnerabilities — Total: 161

| SEVERITY | CVSS V3.0 | VPR SCORE | PLUGIN | NAME |
|---|---|---|---|---|
| CRITICAL | 9.8 | 8.9 | 70728 | Apache PHP-CGI Remote Code Execution |
| CRITICAL | 9.8 | 9.0 | 134862 | Apache Tomcat AJP Connector Request Injection (Ghostcat) |
| CRITICAL | 9.8 | - | 51988 | Bind Shell Backdoor Detection |
| CRITICAL | 9.8 | 6.7 | 184080 | PyTorch TorchServe SSRF (CVE-2023-43654) |
| CRITICAL | 9.8 | - | 20007 | SSL Version 2 and 3 Protocol Detection |
| CRITICAL | 9.8 | 9.7 | 159375 | Spring Cloud Function SPEL Expression Injection (direct check) |
| CRITICAL | 9.8 | 5.9 | 125855 | phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3) |
| CRITICAL | 9.1 | 6.0 | 33447 | Multiple Vendor DNS Query ID Field Prediction Cache Poisoning |
| CRITICAL | 9.0 | 8.1 | 156164 | Apache Log4Shell CVE-2021-45046 Bypass Remote Code Execution |
| CRITICAL | 10.0 | 10.0 | 156016 | Apache Log4Shell RCE detection via Path Enumeration (Direct Check HTTP) |
| CRITICAL | 10.0 | 10.0 | 156056 | Apache Log4Shell RCE detection via Raw Socket Logging (Direct Check) |
| CRITICAL | 10.0 | 10.0 | 156257 | Apache Log4Shell RCE detection via callback correlation (Direct Check DNS) |
| CRITICAL | 10.0 | 10.0 | 156115 | Apache Log4Shell RCE detection via callback correlation (Direct Check FTP) |
| CRITICAL | 10.0 | 10.0 | 156014 | Apache Log4Shell RCE detection via callback correlation (Direct Check HTTP) |
| CRITICAL | 10.0 | 10.0 | 156669 | Apache Log4Shell RCE detection via callback correlation (Direct Check MSRPC) |

| | | | | |
|---|---|---|---|---|
| CRITICAL | 10.0 | 10.0 | 156197 | Apache Log4Shell RCE detection via callback correlation (Direct Check NetBIOS) |
| CRITICAL | 10.0 | 10.0 | 156559 | Apache Log4Shell RCE detection via callback correlation (Direct Check RPCBIND) |
| CRITICAL | 10.0 | 10.0 | 156232 | Apache Log4Shell RCE detection via callback correlation (Direct Check SMB) |
| CRITICAL | 10.0 | 10.0 | 156132 | Apache Log4Shell RCE detection via callback correlation (Direct Check SMTP) |
| CRITICAL | 10.0 | 10.0 | 156166 | Apache Log4Shell RCE detection via callback correlation (Direct Check SSH) |
| CRITICAL | 10.0 | 10.0 | 156162 | Apache Log4Shell RCE detection via callback correlation (Direct Check Telnet) |
| CRITICAL | 10.0 | - | 33850 | Unix Operating System Unsupported Version Detection |
| CRITICAL | 10.0* | 5.1 | 32314 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness |
| CRITICAL | 10.0* | 5.1 | 32321 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) |
| CRITICAL | 10.0* | 5.9 | 11356 | NFS Exported Share Information Disclosure |
| CRITICAL | 10.0* | 7.4 | 46882 | UnrealIRCd Backdoor Detection |
| CRITICAL | 10.0* | - | 61708 | VNC Server 'password' Password |
| HIGH | 8.8 | 7.4 | 164017 | NodeJS System Information Library Command Injection (CVE-2021-21315) |
| HIGH | 8.8 | 7.4 | 19704 | TWiki 'rev' Parameter Arbitrary Command Execution |
| HIGH | 8.6 | 5.2 | 136769 | ISC BIND Service Downgrade / Reflected DoS |
| HIGH | 7.5 | - | 42256 | NFS Shares World Readable |
| HIGH | 7.5 | 6.1 | 42873 | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| HIGH | 7.5 | 5.9 | 90509 | Samba Badlock Vulnerability |
| HIGH | 7.5* | 8.9 | 59088 | PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution |
| HIGH | 7.5* | 6.7 | 36171 | phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4) |
| HIGH | 7.5* | 5.9 | 10205 | rlogin Service Detection |
| HIGH | 7.5* | 5.9 | 10245 | rsh Service Detection |
| MEDIUM | 6.5 | 3.6 | 139915 | ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS |
| MEDIUM | 6.5 | - | 51192 | SSL Certificate Cannot Be Trusted |
| MEDIUM | 6.5 | - | 57582 | SSL Self-Signed Certificate |
| MEDIUM | 6.5 | - | 104743 | TLS Version 1.0 Protocol Detection |
| MEDIUM | 6.5 | - | 42263 | Unencrypted Telnet Server |
| MEDIUM | 5.9 | 4.4 | 136808 | ISC BIND Denial of Service |

| | | | | |
|---|---|---|---|---|
| MEDIUM | 5.9 | 3.6 | 31705 | SSL Anonymous Cipher Suites Supported |
| MEDIUM | 5.9 | 4.4 | 89058 | SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) |
| MEDIUM | 5.9 | 3.6 | 65821 | SSL RC4 Cipher Suites Supported (Bar Mitzvah) |
| MEDIUM | 5.3 | - | 40984 | Browsable Web Directories |
| MEDIUM | 5.3 | 4.0 | 11213 | HTTP TRACE / TRACK Methods Allowed |
| MEDIUM | 5.3 | - | 57608 | SMB Signing not required |
| MEDIUM | 5.3 | - | 15901 | SSL Certificate Expiry |
| MEDIUM | 5.3 | - | 45411 | SSL Certificate with Wrong Hostname |
| MEDIUM | 5.3 | - | 26928 | SSL Weak Cipher Suites Supported |
| MEDIUM | 5.3 | - | 11229 | Web Server info.php / phpinfo.php Detection |
| MEDIUM | 5.0* | - | 11411 | Backup Files Disclosure |
| MEDIUM | 5.0* | - | 46803 | PHP expose_php Information Disclosure |
| MEDIUM | 4.0* | 6.3 | 52611 | SMTP Service STARTTLS Plaintext Command Injection |
| MEDIUM | 4.3* | - | 90317 | SSH Weak Algorithms Supported |
| MEDIUM | 4.3* | 4.5 | 81606 | SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK) |
| MEDIUM | 4.3* | - | 85582 | Web Application Potentially Vulnerable to Clickjacking |
| MEDIUM | 4.3* | 3.8 | 51425 | phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9) |
| MEDIUM | 5.0* | - | 36083 | phpMyAdmin file_path Parameter Vulnerabilities (PMASA-2009-1) |
| MEDIUM | 4.3* | 3.0 | 49142 | phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7) |
| LOW | 3.7 | 3.6 | 70658 | SSH Server CBC Mode Ciphers Enabled |
| LOW | 3.7 | - | 153953 | SSH Weak Key Exchange Algorithms Enabled |
| LOW | 3.7 | 4.5 | 83875 | SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) |
| LOW | 3.7 | 4.5 | 83738 | SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam) |
| LOW | 3.4 | 5.1 | 78479 | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) |
| LOW | 2.6* | - | 71049 | SSH Weak MAC Algorithms Enabled |
| LOW | N/A | - | 42057 | Web Server Allows Password Auto-Completion |
| LOW | 2.6* | - | 26194 | Web Server Transmits Cleartext Credentials |
| LOW | 2.6* | - | 10407 | X Server Detection |
| INFO | N/A | - | 10114 | ICMP Timestamp Request Remote Date Disclosure |
| INFO | N/A | - | 10223 | RPC portmapper Service Detection |
| INFO | N/A | - | 21186 | AJP Connector Detection |
| INFO | N/A | - | 18261 | Apache Banner Linux Distribution Disclosure |

A titolo esemplificativo ho incollato le criticità emerse fino al livello “low” poiché la macchina Metasploitable è nata per essere attaccata e, per sua natura, presenta molte criticità.

Prenderò come esempio cinque vulnerabilità di livello diverso per analizzare ogni grado di rischio.

| | | | | |
|---|---|---|---|---|
| CRITICAL | 10.0 | 10.0 | 156115 | Apache Log4Shell RCE detection via callback correlation (Direct Check FTP) |

## Synopsis

The version of Apache Log4j used on the remote server is affected by a remote code execution vulnerability.

## Description

A remote code execution vulnerability exists in Apache Log4j < 2.15.0 due to insufficient protections on message lookup substitutions when dealing with user controlled input. A remote, unauthenticated attacker can exploit this, via a web request to execute arbitrary code with the permission level of the running Java process.

## Solution

Upgrade to Apache Log4j version 2.15.0 or later, or apply the vendor mitigation.

Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions / patches have known high severity vulnerabilities and the vendor is updating their advisories often as new research and knowledge about the impact of Log4j is discovered. Refer to https://logging.apache.org/log4j/2.x/security.html for the latest versions.

## See Also

https://logging.apache.org/log4j/2.x/security.html

https://www.lunasec.io/docs/blog/log4j-zero-day/

## Plugin Details

**Severity:** Critical

**ID:** 156115

**File Name:** log4j_log4shell_ftp.nbin

**Version:** 1.67

**Type:** remote

**Family:** FTP

**Published:** 12/16/2021

**Updated:** 2/22/2024

**Supported Sensors:** Nessus

## Risk Information

### VPR

**Risk Factor:** Critical

**Score:** 10.0

### CVSS v2

**Risk Factor:** High

**Base Score:** 9.3

**Temporal Score:** 8.1

Sinossi:

La versione di Apache Log4j utilizzata sul server remoto è affetta da una vulnerabilità di esecuzione remota del codice.

Descrizione:

Una vulnerabilità di esecuzione remota del codice esiste in Apache Log4j < 2.15.0 a causa di protezioni insufficienti sulle sostituzioni di ricerca dei messaggi quando si gestisce l'input controllato dall'utente. Un attaccante remoto e non autenticato può sfruttare questo, tramite una richiesta web, per eseguire codice arbitrario con il livello di autorizzazione del processo Java in esecuzione.

Soluzione:

Aggiornare alla versione 2.15.0 o successiva di Apache Log4j, o applicare la mitigazione del fornitore.

Si consiglia vivamente di aggiornare alle versioni più recenti di Apache Log4j poiché le versioni intermedie/patch hanno vulnerabilità conosciute di gravità elevata e il fornitore aggiorna spesso i propri avvisi man mano che vengono scoperte nuove ricerche e conoscenze sull'impatto di Log4j. Fare riferimento a https://logging.apache.org/log4j/2.x/security.html per le ultime versioni.

Vedi anche:

https://logging.apache.org/log4j/2.x/security.html

https://www.lunasec.io/docs/blog/log4j-zero-day/

*Commento della vulnerabilità:*

*Questa vulnerabilità, che è presente nel servizio di logger Apache log4j, permette all'attaccante di eseguire del codice malevolo da remoto. Attraverso l'aggiornamento della versione di Apache log4j è stata risolta questa vulnerabilità.*


## Synopsis

An SMB server running on the remote host is affected by the Badlock vulnerability.

## Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

## Solution

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

## See Also

http://badlock.org

https://www.samba.org/samba/security/CVE-2016-2118.html

## Plugin Details

**Severity:** High

**ID:** 90509

**File Name:** samba_badlock.nasl

**Version:** 1.8

**Type:** remote

**Family:** General

**Published:** 4/13/2016

**Updated:** 11/20/2019

**Supported Sensors:** Nessus

## Risk Information

**VPR**

**Risk Factor:** Medium

**Score:** 5.9

**CVSS v2**

**Risk Factor:** Medium

**Base Score:** 6.8

**Temporal Score:** 5

**Vector:** CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P

Sinossi

Un server SMB in esecuzione sull'host remoto è interessato dalla vulnerabilità Badlock.

Descrizione

La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è interessata da una falla, nota come Badlock, che esiste nei protocolli Security Account Manager (SAM) e Local Security Authority (Domain Policy) (LSAD) a causa di una negoziazione del livello di autenticazione impropria sui canali di chiamata di procedura remota (RPC). Un attaccante uomo-in-the-middle che è in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare un abbassamento del livello di autenticazione, il che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come

visualizzare o modificare dati sensibili di sicurezza nel database Active Directory (AD) o disabilitare servizi critici.

Soluzione

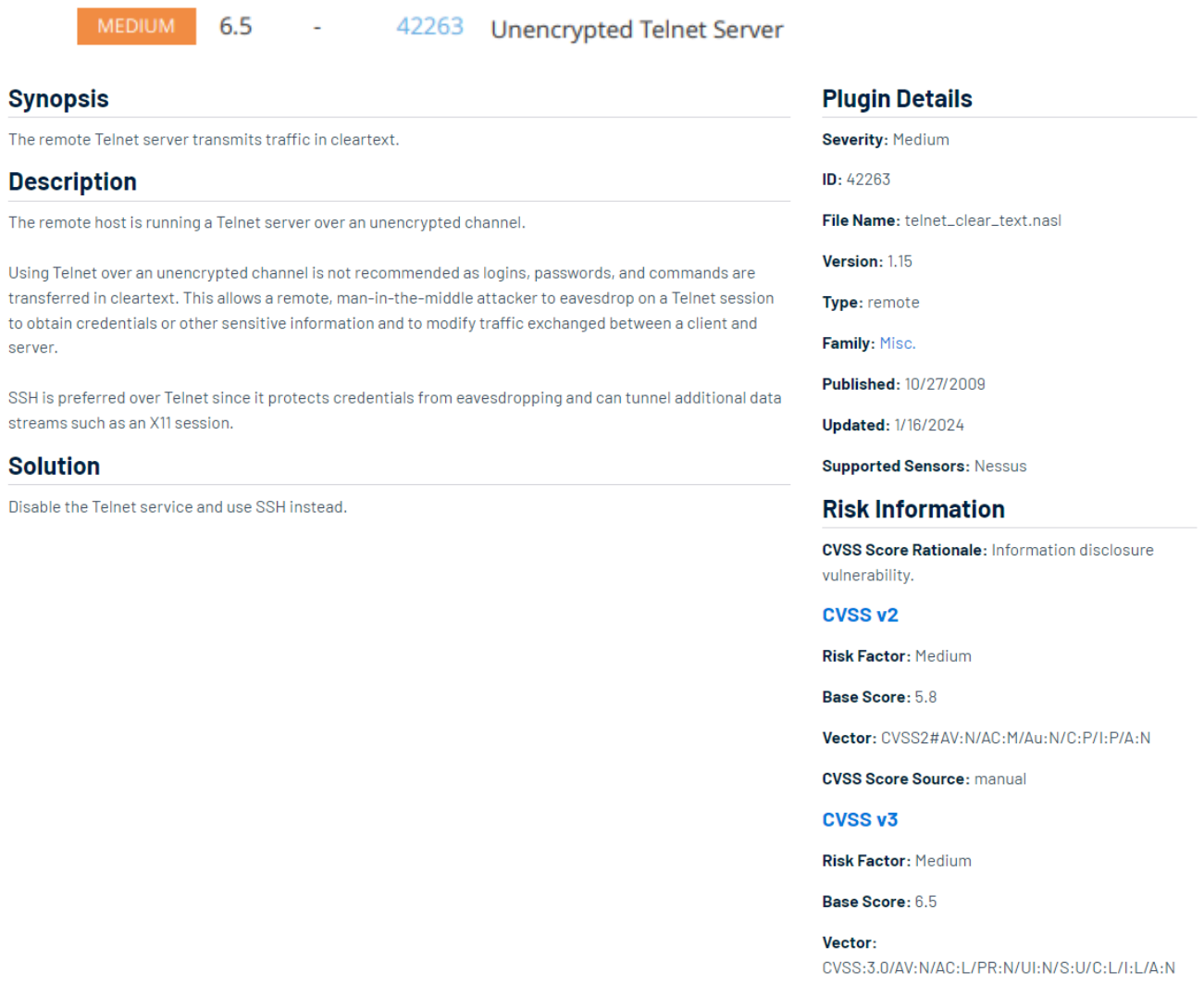
Aggiornare alla versione di Samba 4.2.11 / 4.3.8 / 4.4.2 o successiva.

Vedi anche
http://badlock.org

https://www.samba.org/samba/security/CVE-2016-2118.html

*Commento della vulnerabilità:*

*Il server Samba è potenzialmente vulnerabile ad un attacco man-in-the-middle che sfrutta una falla presente nei protocolli SAM e LSAD. Con l'aggiornamento della versione Samba viene risolta questa vulnerabilità.*




Sinossi

Il server Telnet remoto trasmette il traffico in testo non cifrato.

Descrizione

L'host remoto sta eseguendo un server Telnet su un canale non crittografato. L'utilizzo di Telnet su un canale non crittografato non è consigliato poiché i login, le password e i comandi vengono trasferiti in testo non cifrato. Ciò consente a un attaccante remoto uomo-in-the-middle di intercettare una sessione Telnet per ottenere credenziali o altre informazioni sensibili e di modificare il traffico scambiato tra un client e un server.

SSH è preferibile rispetto a Telnet poiché protegge le credenziali dall'intercettazione e può instradare flussi di dati aggiuntivi come una sessione X11.

Soluzione

Disabilitare il servizio Telnet e utilizzare invece SSH.

*Commento della vulnerabilità:*

*Il servizio Telnet non utilizza alcuna crittografia pertanto il servizio potrebbe essere vulnerabile da un attacco man-in-the-middle. La soluzione proposta è quella del cambio di strumento per questo servizio.*

CRITICAL 9.8 - 51988 Bind Shell Backdoor Detection

## Synopsis

The remote host may have been compromised.

## Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

## Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

## Plugin Details

**Severity:** Critical

**ID:** 51988

**File Name:** wild_shell_backdoor.nasl

**Version:** 1.10

**Type:** remote

**Family:** Backdoors

**Published:** 2/15/2011

**Updated:** 4/11/2022

**Configuration:** Enable thorough checks

**Supported Sensors:** Nessus

## Risk Information

**CVSS Score Rationale:** Score based on manual analysis

### CVSS v2

**Risk Factor:** Critical

**Base Score:** 10

**Vector:** CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

**CVSS Score Source:** manual

Sinossi

L'host remoto potrebbe essere stato compromesso.

Descrizione

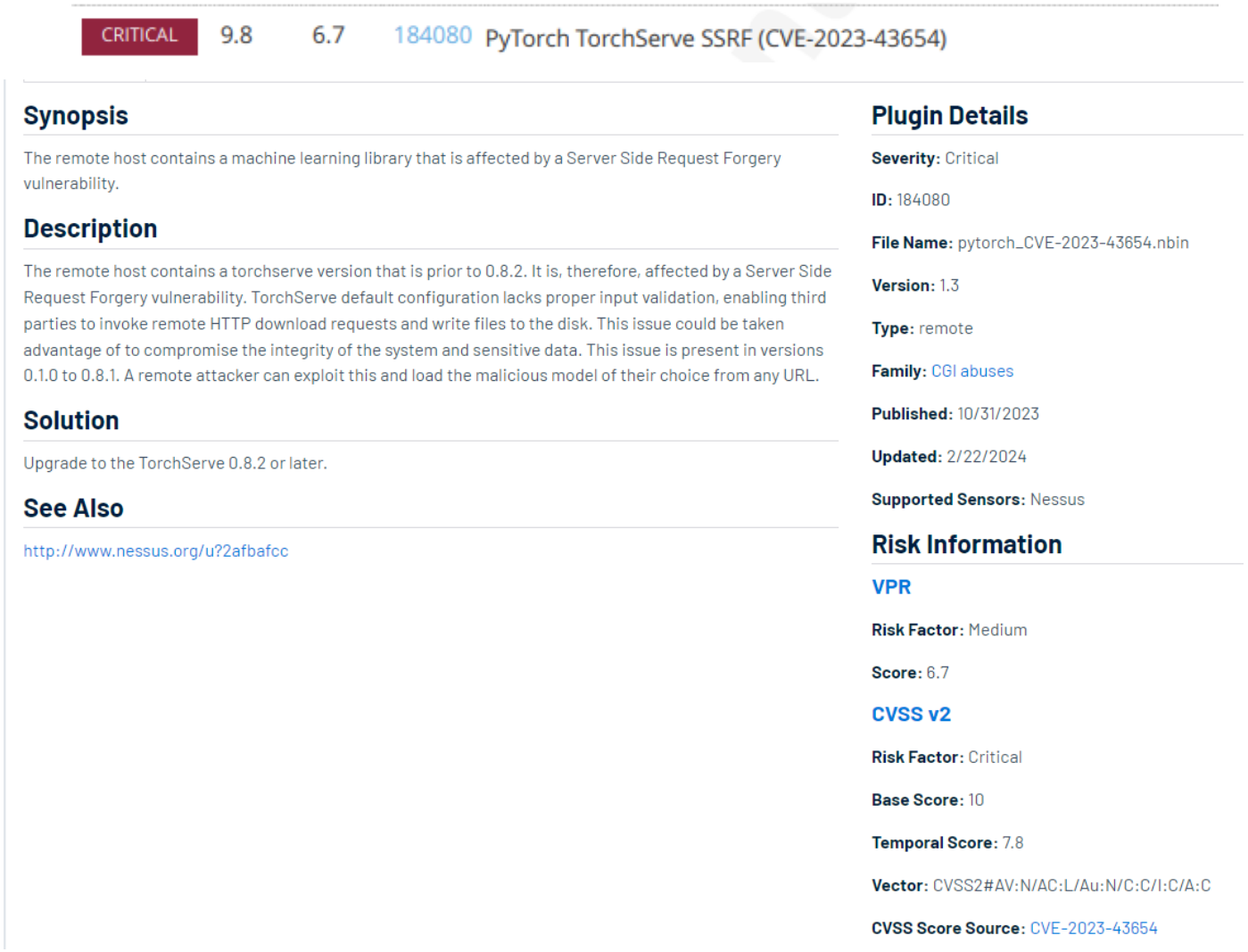
Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un attaccante potrebbe utilizzarla collegandosi alla porta remota e inviando comandi direttamente.

Soluzione

Verificare se l'host remoto è stato compromesso e reinstallare il sistema se necessario.

*Commento della vulnerabilità:*

*Questa vulnerabilità ci evidenzia che una shell è in ascolto su una porta remota senza che sia richiesta alcuna autenticazione e la soluzione proposta è drastica; viene consigliato di reinstallare il sistema.*




Sinossi

L'host remoto contiene una libreria di machine learning che è interessata da una vulnerabilità di Forgery delle Richieste Lato Server.

Descrizione

L'host remoto contiene una versione di torchserve precedente alla 0.8.2. Pertanto, è interessato da una vulnerabilità di Forgery delle Richieste Lato Server. La configurazione predefinita di TorchServe manca di una valida validazione dell'input, consentendo a terze parti di invocare richieste di download HTTP remote e scrivere file sul disco. Questo problema potrebbe essere sfruttato per compromettere l'integrità del sistema e dei dati sensibili. Questo problema è presente nelle versioni da 0.1.0 a 0.8.1. Un attaccante remoto può sfruttare questo e caricare il modello maligno di sua scelta da qualsiasi URL.

Soluzione

Aggiornare alla versione di TorchServe 0.8.2 o successiva.

Vedi Anche

http://www.nessus.org/u?2afbafcc

*Commento della vulnerabilità:*

*L'host remoto ha una libreria di machine learning vulnerabile alla manipolazione delle richieste dal lato server. La soluzione è aggiornare a torchserve 0.8.2 o successivo.*