04/02/2022

cybersecurity360.it

Argomento: Exprivia: si parla di noi

EAV: € 1.521
Utenti unici: 28.467

https://www.cybersecurity360.it/nuove-minacce/vulnerabilita-in-samba-permettono-di-prendere-il-controllo-dei-server-esposti-come-mitigare-il-rischio/

Vulnerabilità in Samba permettono di prendere il controllo dei server esposti: come mitigare il rischio

Tre falle affliggono Samba, di cui una critica e un'altra ad alta gravità. In particolare, attaccanti remoti possono sfruttarle per eseguire codice arbitrario, scalando privilegi da root, e prendere il controllo dei server che eseguono il software vulnerabile. I consigli degli esperti per proteggersi

Samba richiede un aggiornamento immediato. Tre vulnerabilità affliggono l'implementazione open source del protocollo SMB. Una vulnerabilità è critica e un'altra è ad alta gravità. "Samba è un protocollo Server Message Block (SMB), che permette la condivisione di risorse (file, stampanti, ecc) tra sistemi operativi diversi (Windows che deve comunicare in rete con Linux); perciò permette interoperabilità tra Linux, Unix, macOS e Windows", commenta Rosita Galiandro, Responsabile Osservatorio Exprivia sulla cybersecurity.

Indice degli argomenti

Cos'è Samba e perché preoccupa la falla

"La falla CVE-2021-44142 (valutata 9.9 sulla scala CVSS) nel progetto Samba è estremamente preoccupante", commenta Pierluigi Paganini, analista di cyber security e CEO Cybhorus. Ed è allarmante "in primis per l'ampia diffusione del progetto da parte di organizzazioni di ogni dimensione in tutto il mondo".

"Ricordiamo", continua Paganini, "che il progetto nasce per fornire servizi di condivisione di file e stampanti ed è un elemento cruciale per garantire interoperabilità tra sistemi Unix, Linux, macOS e Windows".

Infatti, Server Message Block (SMB) è un protocollo di networking che trova impiego nella condivisione in rete di file, porte e

stampanti attraverso diverse piattaforme. Parlando di Linux, la falla affligge le distribuzioni Red Hat, SUSE Linux e Ubuntu.

I dettagli tecnici della vulnerabilità in Samba

"Recentemente alcune vulnerabilità su Samba hanno attirato l'attenzione degli esperti", prosegue Rosita Galiandro, che ci illustra tutti i dettagli tecnici della falla: "In ordine di criticità proviamo a descriverle per identificare azioni di contenimento del rischio. "La vulnerabilità con gravità più 'critica' è CVE-2021-44142, valutata 9,9 su 10 (scala CVSS) , ha un impatto su tutte le versioni di Samba precedenti alla 4.13.17″, continua Galiandro: "Riguarda una vulnerabilità "out-of-bounds heap read/write" che si verifica nel modulo VFS (Virtual File System) chiamato vfs_fruit durante il processo di analisi dei metadati EA quando si apre un file in Samba (smbd). Il modulo vfs_fruit è progettato per fornire l'interoperabilità tra Samba e Netatalk".

"Netatalk è un'implementazione dell'Apple Filing Protocol (AFP) che consente ai sistemi simili a Unix di fungere da file server per i dispositivi Apple. Questa vulnerabilità consente agli attaccanti remoti di divulgare informazioni riservate e l'esecuzione arbitraria di codice sulle installazioni infette di Samba. In particolare, le falle sono presenti all'interno delle funzioni fruit_pread e fruit_pwrite. Nella prima il problema deriva dalla mancanza di un'adeguata convalida dei dati forniti dall'utente, che può comportare una lettura oltre la fine di un buffer allocato. Nella seconda il problema deriva dalla mancanza di un'adeguata convalida della lunghezza dei dati forniti dall'utente prima di copiarli in un buffer basato su heap a lunghezza fissa", sottolinea l'esperta di cybersecurity.

Il problema interessa tutte le versioni di Samba

Il problema affligge tutte le release di Samba, comprese quelle "precedenti alla 4.13.17", mette in guardia Rosita Galiandro, "che adottano una configurazione predefinita del modulo VFS fruit. Infatti, ha spiegato il team di sicurezza di Samba, che in esso sono presenti due impostazioni predefinite: fruit:metadata=netatalk o fruit:resource=file che sono la causa della criticità.

Se entrambe le opzioni sono impostate su valori diversi rispetto a quelli indicati, il sistema è al sicuro e non è vulnerabile ad eventuali attacchi di sicurezza". Continua Galiandro: "Per sfruttare questa vulnerabilità è necessario l'accesso in scrittura agli attributi estesi di un file da parte dell'utente. Secondo il team di Samba, bisogna tenere presente che in questi casi potrebbe trattarsi di un utente guesto non autenticato. Pertanto, l'autenticazione non è indispensabile per sfruttare questa vulnerabilità".

Le altre falle in Samba

"Gravità 'alta' ha invece la CVE-2021-44141", sottolinrea Galiandro: "A causa di questa vulnerabilità ci può essere una perdita di informazioni tramite collegamenti simbolici dell'esistenza di file o directory al di fuori della condivisione esportata. Un collegamento simbolico (Symlink) serve per indirizzare verso un file specifico o per "ingannare" programmi ed utenti". "La vulnerabilità meno grave, ma non trascurabile, è la CVE-2022-0336 che consente agli utenti di Samba Active Directory (AD), con il permesso di scrittura, di impersonare servizi arbitrari. Un utente malintenzionato, che ha la capacità di scrivere su un profilo, può sfruttare l'exploit per eseguire un attacco Denial of Service (DoS)

aggiungendo qualsiasi Service Principals Names (SPN) che corrisponde a un servizio esistente. Inoltre, un attaccante in grado di intercettare il traffico può impersonare i servizi esistenti, con conseguente perdita di riservatezza e integrità.

Cosa preoccupa gli esperti

"Uno degli aspetti più preoccupanti relativi alla vulnerabilità in questione", sottolinea Paganini, "è che essa può essere sfruttata in attacchi relativamente semplici ed inoltre non richiede alcuna iterazione dell'utente".

Infatti, attaccanti possono sfruttare una vulnerabilità critica per eseguire codice arbitrario con privilegi da root sulle installazioni infette. In particolare, la falla CVE-2021-44142 impatta tutte le versioni di Samba prima della release 4.13.17, vulnerabili alla falla "out-of-bounds heap read write" presente nel modulo VFS (vfs_fruit), quando analizza i metadati EA, aprendo file in smbd.

"Lo scenario descritto è quanto di peggio possa accadere ad una infrastruttura in cui sono presenti uno o più sistemi che eseguono una versione di Samba affetta dalla falla", conclude Paganini.

Come mitigare il rischio

Samba ha rilasciato l'aggiornamento software da applicare, per sanare le molteplici vulnerabilità a rischio exploit.

Gli amministratori di sistema devono subito aggiornare il protocollo alle versioni 4.13.17, 4.14.12 o 4.15.5 o risolvere la falla ricorrendo alle security patch già distribuite.

Per proteggersi, è necessario eseguire gli aggiornamenti di sicurezza o disabilitare il modulo vfs_fruit, ci spiega Galiandro: "Il rischio è elevato in quanto è evidente come gli attaccanti possono sfruttare in modo semplice l'exploit senza bisogno dell'interazione dell'utente, se i server presi di mira eseguono installazioni di Samba precedenti alla versione 4.13.17".

Ecco i consigli dell'esperta di cybersecurity: "Si raccomanda di eseguire l'aggiornamento alle versioni 4.13.17, 4.14.12 o 4.15.5 o di applicare, il prima possibile, le patch di sicurezza rilasciate da Samba per mitigare la falla e contrastare qualsiasi potenziale attacco che sfrutti queste vulnerabilità. Come soluzione alternativa, è consigliabile rimuovere il modulo VFS fruit dall'elenco degli oggetti VFS configurati in qualsiasi rigo vfs objects nella configurazione di Samba smb.conf. Si noti che la modifica delle impostazioni del modulo VFS fruit:metadata o fruit:resource, per utilizzare l'impostazione non infetta, renderebbe inaccessibili tutte le informazioni archiviate nel server. Inoltre, considerando che il protocollo Samba (SMB) fornisce l'interoperabilità tra i sistemi, è consigliato monitorare le trasmissioni di dati condivisi (file e stampanti) e la condivisione degli accessi".

"Infine, il protocollo Samba, utilizzato per i servizi remoti, può essere utilizzato in modo improprio dagli aggressori per propagarsi attraverso la rete dell'organizzazione o utilizzato come punto di partenza per diffondersi ad altri sistemi connessi. Si consiglia, pertanto, di monitorare e scansionare le trasmissioni che richiedono le configurazioni vfs_fruit", conclude Rosita Galiandro.