



Esercizio WannaCry

WannaCry è un tipo di ransomware che sfrutta una vulnerabilità di Windows nota come EternalBlue per propagarsi all'interno di una rete. Questa vulnerabilità era presente nelle versioni non aggiornate di Windows e permetteva al malware di propagarsi su reti collegate, senza richiedere l'interazione dell'utente. L'exploit EternalBlue era inizialmente una tool di hacking sviluppato dalla National Security Agency (NSA) degli Stati Uniti. Tuttavia, è stato rubato e successivamente utilizzato da gruppi di cybercriminali, incluso il gruppo responsabile di WannaCry. Una volta che WannaCry si è infiltrato in un sistema, ha crittografato i file presenti sulla macchina, rendendoli inaccessibili agli utenti. Successivamente, il malware visualizzava un messaggio di richiesta di riscatto, chiedendo alle vittime di pagare una somma di denaro in bitcoin per ottenere la chiave di decrittazione. Il ransomware cercava di intimidire le vittime con minacce di eliminare definitivamente i file se il riscatto non veniva pagato entro un determinato periodo di tempo.





CVE List • CNAs • WGs • Board • About • News & Blog •



Go to for:
CVE Sources
CVE Info

Search CVE List • Downloads • Data Feeds • Update a CVE Record • Request CVE IDs

TOTAL CVE Records: 223313

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Legacy CVE download formats deprecation is now underway and will end on June 30, 2024. New CVE List download format is available now.

HOME > CVE > CVE-2017-0144

CVE-ID

CVE-2017-0144 [Learn more at National Vulnerability Database \(NVD\)](#)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description
The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

References

[Printer-Friendly View](#)

CVE-2017-0144 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

QUICK INFO

CVE Dictionary Entry:

CVE-2017-0144

NVD Published Date:

03/16/2017

NVD Last Modified:

06/20/2018

Source:

Microsoft Corporation

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: **8.1 HIGH**

Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

Fatte le dovute premesse passiamo ora ad ipotizzare uno scenario in cui abbiamo una rete, nella quale sono connessi 30 host, e uno di questi sia un Win7 infetto da WannaCry. Analizzeremo quindi gli interventi tempestivi sulla macchina infetta e le varie possibilità della messa in sicurezza del sistema, supponendo che non sia disponibile la patch di sicurezza.

Interventi su macchina infetta

- **Isolamento della macchina:** Come prima, è essenziale isolare immediatamente il PC infetto dalla rete per prevenire la propagazione del malware, disconnettendolo fisicamente dalla rete.
- **Analisi approfondita:** Condurre un'analisi approfondita del sistema infetto per identificare il malware e le sue modalità di esecuzione.

Possibilità di messa in sicurezza degli altri PC

- **Isolamento preventivo:** Isolare preventivamente gli altri PC disconnettendoli dalla rete finché non è possibile garantire la sicurezza.
- **Monitoraggio del traffico:** Implementare sistemi di monitoraggio del traffico di rete per rilevare eventuali tentativi di propagazione del malware.
- **Spegnimento dei sistemi:** Spegnerne i sistemi non essenziali per ridurre la superficie di attacco e limitare la diffusione del malware.
- **Implementare filtri di rete:** Configurare filtri di rete per bloccare il traffico sospetto e limitare la comunicazione con indirizzi IP noti associati a WannaCry.
- **Formazione degli utenti:** Rafforzare la formazione degli utenti sull'importanza di evitare clic su link e apertura di allegati sospetti.
- **Backup offline:** Assicurarsi che i backup siano offline o altrimenti inaccessibili al malware per evitare la cifratura dei dati di backup.

Pro e contro delle misure di sicurezza

Pro dell'isolamento preventivo: Riduce il rischio di diffusione. Tuttavia, può interrompere temporaneamente le operazioni aziendali.

Pro del monitoraggio del traffico: Permette la rilevazione tempestiva di attività sospette. Tuttavia, potrebbe richiedere risorse dedicate.

Pro dell'implementazione di filtri di rete: Riduce la possibilità di comunicazione con server di controllo e diffusione del malware. Tuttavia, può richiedere configurazioni e manutenzione aggiuntive.

Contro dello spegnimento dei sistemi: Potrebbe interrompere le attività aziendali. Tuttavia, riduce la superficie di attacco.

Contro della formazione degli utenti: Ancora difficile eliminare completamente il rischio umano. Tuttavia, la formazione riduce la probabilità di azioni inconsapevoli.

Conclusioni

In assenza di una patch, l'approccio principale è prevenire la diffusione e mitigare il rischio attraverso l'isolamento e la riduzione delle opportunità di propagazione.