HC3: Sector Alert

May 10, 2023 TLP:CLEAR Report: 202305101500

Veeam Backup & Replication Latest Threat Actor Target

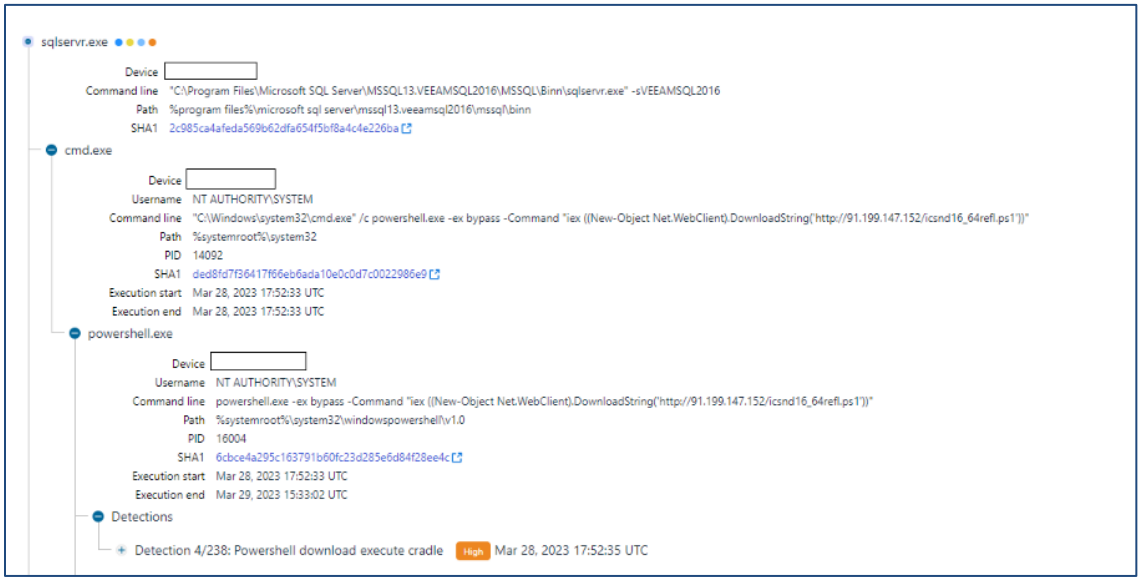
Executive Summary

Cyber attacks launched by threat actors against Veeam Backup & Replication are on the rise. Veeam Backup & Replication (VBR) is a software product created by Veeam Software that is used to back up, replicate, and restore data on virtual machines (VMs). What makes this threat significant is that in addition to backing up and recovering VMs, it is used to protect and restore individual files and applications for environments such as Microsoft Exchange and SharePoint, which are used in the HPH sector. Veeam Backup & Replication also has the ability to provide transaction-level restores of Oracle and Microsoft SQL databases. HC3 recommends that all HPH sector entities be aware of suspicious activity, keep systems up to date, and immediately patch any vulnerable systems.

Report

In late March 2023, threat researchers identified attacks carried out by at least one threat actor group, FIN7, against internet-facing servers running Veeam Backup & Replication software. FIN7 is a threat actor group that was discovered in the mid-2010s. The cybercrime group is financially motivated, has been connected to numerous high-profile attacks, and their evolution includes developing new tools, and expanding their operations. FIN7 is known for affiliating with other threat actor groups such as Conti, REvil, and BlackBasta.

On March 28th, malicious activity similar to FIN7 was observed across internet-facing servers running Veeam Backup & Replication software. A SQL server process written as “sqlservr.exe” related to the Veeam Backup instance executed a shell command, which performed in-memory download and execution of a PowerShell script. According to threat researchers, based on the timing of the campaign, open TCP port 9401 on compromised servers, and the hosts running a vulnerable version of VBR, the researchers believe that the intruder likely exploited the CVE-2023-27532 vulnerability for access and malicious code execution.



Example of shell command launched using sqlserver.exe. *Source: WithSecure*

Tracked as CVE-2023-27532, this high-severity vulnerability exposes encrypted credentials that are stored

in the VBR configuration to unauthenticated users in the backup infrastructure, which could lead to unauthorized access to the backup infrastructure hosts. While the intention behind this attack is not clear, the intrusions could have ended with data theft or deployment of ransomware if the attack chain completed successfully.

On March 7th, Veeam Software addressed this issue and provided workaround instructions. However, on March 23rd, a pentesting company released an exploit for CVE-2023-27532 that demonstrated how an unsecured API endpoint can be abused to extract the credentials in plain text. If successful, a threat actor could leverage this vulnerability to run code remotely with the highest privileges. What is significant about this is that threat researchers determined that approximately 7,500 internet-exposed VBR hosts appeared to be vulnerable.

Patches, Mitigations, and Workarounds

According to the vendor, Veeam Software, the vulnerability CVE-2023-27532 affects all Veeam Backup & Replication versions. HC3 recommends that all users adhere to Veeam's guidance regarding Veeam Backup & Replication, which are the following:

- If using an earlier Veeam Backup & Replication version, please upgrade to a supported version first, which can be found here.
- If you use an all-in-one Veeam appliance with no remote backup infrastructure components, you can alternatively block external connections to port TCP 9401 in the backup server firewall as a temporary remediation until the patch is installed.
- The patch must be installed on the Veeam Backup & Replication server. All new deployments of Veeam Backup & Replication versions 12 and 11a installed using the ISO images dated February 23, 2023 (V12) and February 27, 2023 (V11a) or later are not vulnerable.

HC3 recommends that all HPH sector entities remain vigilant and aware of suspicious activity, keep systems up to date, and immediately patch any vulnerable systems. In addition to this, organizations are encouraged to take a proactive approach by using CISA's free cybersecurity services and tools to strengthen their cyber posture.

References

CISA: Free Cybersecurity Services and Tools
https://www.cisa.gov/free-cybersecurity-services-and-tools

Ex-Conti and FIN7 Actors Collaborate with New Backdoor
https://securityintelligence.com/posts/ex-conti-fin7-actors-collaborate-new-backdoor/

Ex-Conti members and FIN7 devs team up to push new Domino malware
https://www.bleepingcomputer.com/news/security/ex-conti-members-and-fin7-devs-team-up-to-push-new-domino-malware/

Hackers target vulnerable Veeam backup servers exposed online
https://www.bleepingcomputer.com/news/security/hackers-target-vulnerable-veeam-backup-servers-exposed-online/

HC3: Sector Alert

May 10, 2023 TLP:CLEAR Report: 202305101500

Huntress Labs: Veeam Backup & Replication CVE-2023-27532 Response
https://www.huntress.com/blog/veeam-backup-replication-cve-2023-27532-response

Veeam makes products for the health sector (we know because some of them are HIPAA compliant)
https://www.veeam.com/healthcare-data-availability-solutions.html

Veeam's knowledge base article for more details:
https://www.veeam.com/kb4424

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback