

FIN7 Hackers Caught Exploiting Recent Veeam Vulnerability

Russian cybercrime group FIN7 has been observed exploiting unpatched Veeam Backup & Replication instances in recent attacks, cybersecurity company WithSecure reports.

Around since at least 2015 and also referred to as Anunak, and Carbanak, FIN7 is a financially motivated group mainly focused on credit card information theft. Security researchers believe there are numerous sub-groups operating under the FIN7 umbrella.

Over the past years, some of the threat actors overlapping with FIN7 operations were seen transitioning to ransomware, including REvil, DarkSide, BlackMatter, Alphv, and Black Basta.

At the end of March 2023, WithSecure caught FIN7 attacks that exploited internet-facing servers running Veeam Backup & Replication software to execute payloads on the compromised environment.

The cybersecurity firm observed a Veeam Backup process executing a shell command to download and execute a PowerShell script that turned out to be the Powertrash in-memory dropper known to be used by FIN7.

The dropper was used to drop Diceloder, a backdoor also known as Lizar, which enables attackers to perform various post-exploitation operations, and which has been linked to FIN7 before.

“The exact method used by the threat actor to invoke the initial shell commands remains unknown but was likely achieved through a recently patched Veeam Backup & Replication vulnerability, CVE-2023-27532, which can provide unauthenticated access to a Veeam Backup & Replication instance,” WithSecure says.

CVE-2023-27532 (CVSS score of 7.5) was disclosed and patched in early March. Roughly two weeks later, proof-of-concept (PoC) exploitation code targeting the vulnerability was released publicly.

According to Veeam, successful exploitation of the bug allows an attacker to obtain encrypted credentials that are stored in the configuration database. However, penetration testing firm Horizon3.ai, which released the PoC, says that the flaw allows attackers to obtain cleartext credentials.

As part of the observed FIN7 attacks, WithSecure identified suspicious activity targeting the exploited Veeam backup instances days before payloads were dropped, likely to probe and identify vulnerable servers.

The threat actor was seen performing network reconnaissance, stealing information from the Veeam backup database, exfiltrating stored credentials, achieving persistence for the Diceloder backdoor, and moving laterally using the stolen credentials.

“WithSecure Intelligence has so far identified two instances of such attacks conducted by FIN7. As the initial activity across both instances were initiated from the same public IP address on the same day, it is likely that these incidents were part of a larger campaign. However, given the probable rarity of Veeam backup servers with TCP port 9401 publicly exposed, we believe the scope of this attack is limited,” WithSecure notes.

CVE-2023-27532 was addressed with the release of Veeam Backup

& Replication versions 12 (build 12.0.0.1420 P20230223) and 11a (build 11.0.1.1261 P20230227), which organizations need to install on the Veeam Backup & Replication server.

Vulnerabilities in Veeam's product have been exploited in previous attacks and organizations are advised to update their Backup & Replication instances as soon as possible.

Related: CISA Warns Veeam Backup & Replication Vulnerabilities Exploited in Attacks

Related: New 'Domino' Malware Linked to FIN7 Group, Ex-Conti Members

Related: FIN7 Cybercrime Operation Continues to Evolve Despite Arrests

FIN7 Hackers Caught Exploiting Recent Veeam Vulnerability