

PoC Exploit Published for Just-Patched Veeam Data Backup Solution Flaw

Security researchers have published proof-of-concept (PoC) code that provides a roadmap to exploit a recently patched high-severity vulnerability in the Veeam Backup & Replication product

Earlier this month, Veeam released a patch for CVE-2023-27532 (CVSS score of 7.5), a security defect the company warned could be exploited to obtain encrypted credentials that are stored in the configuration database.

Successful exploitation of the issue, Veeam said, could allow an attacker to access the backup infrastructure hosts. Unpatched publicly exposed Veeam instances with a TCP port 9401 open could become easy targets to attackers.

A few days after Veeam's patch release, anti-malware company Huntress said that there might be thousands of hosts running vulnerable versions of the solution, urging users to update their installations as soon as possible.

Patching is now critical, as Horizon3.ai has released proof-of-concept code targeting the flaw, along with a technical writeup of the vulnerability and the exploitation process.

"CVE-2023-27532 allows an unauthenticated user with access to the Veeam backup service to request cleartext credentials. We have examined the vulnerable port, reverse engineered the Veeam Backup Service, and constructed a WCF client using .NET core," Horizon3.ai warned.

The vulnerability 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 need to be installed on the Veeam Backup & Replication server.

While there are no reports of CVE-2023-27532 being exploited in attacks, it might not be long before exploitation begins. Threat actors have been known to target Backup & Replication flaws in their attacks.

Veeam Backup & Replication is a backup solution for virtual environments that offers support for cloud-based workloads servers, and workstations, and for Hyper-V, Nutanix AHV, and vSphere virtual machines.

Related: Exploitation of Oracle E-Business Suite Flaw Starts After PoC Publication

Related: Exploitation of Control Web Panel Vulnerability Starts After PoC Publication

Related: PoC Code Published for High-Severity macOS Sandbox Escape Vulnerability

PoC Exploit Published for Just-Patched Veeam Data Backup Solution Flaw