CERT-EU

Security Advisory 2023-016

High Vulnerability in Veeam Backup & Replication

March 09, 2023 — v1.0

TLP:CLEAR

History:

- *09/03/2023 — v1.0 – Initial publication*

Summary

On March 8, 2023, Veeam released a new security advisory revealing one high vulnerability in a Veeam Backup & Replication component [1]. This vulnerability is identified by `CVE-2023-27532` (CVSS score of 7.5) and it may allow an attacker to obtain encrypted credentials stored in the configuration database. This may lead to gaining access to the backup infrastructure hosts.

It is highly recommended installing the latest version.

Technical Details

The `CVE-2023-27532` is caused by the vulnerable process `Veeam.Backup.Service.exe` (TCP 9401 by default) that allows an unauthenticated user to request encrypted credentials.

Affected Products

This vulnerability affects all Veeam Backup & Replication versions.

All new deployments of Veeam Backup & Replication versions 12 and 11 installed using the ISO images dated `20230223` (V12) and `20230227` (V11) or later are not vulnerable.

Recommendations

It is highly recommended updating to a supported [2] and fixed version:

- Version 12 (build 12.0.0.1420 P20230223) [3];
- Version 11a (build 11.0.1.1261 P20230227) [4].

Workarounds

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.

References

[1] https://www.veeam.com/kb4424

[2] https://www.veeam.com/product-lifecycle.html?ad=in-text-link

[3] https://www.veeam.com/kb4420?ad=in-text-link

[4] https://www.veeam.com/kb4245?ad=in-text-link