Vulnerability has been discovered within a Veeam® Backup & Replication™ component that could allow an unauthenticated user access

2023-03-10 - Aleksejs Vasiļevskis - Comments (0) - General

Challenge

Vulnerability CVE-2023-27532 in Veeam Backup & Replication component allows to obtain encrypted credentials stored in the configuration database. This may lead to gaining access to the backup infrastructure hosts.

Severity: High

CVSS v3 score: 7.5

Cause

The vulnerable process, Veeam.Backup.Service.exe (TCP 9401 by default), allows an unauthenticated user to request encrypted credentials.

Solution

This vulnerability is resolved in the following Veeam Backup & Replication versions:

- 12 *(build 12.0.0.1420 P20230223)*
- 11a *(build 11.0.1.1261 P20230227)*

Notes:

- This vulnerability affects all Veeam Backup & Replication versions.
- If you use an earlier Veeam Backup & Replication version, please upgrade to a supported version first.
- 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 11 installed using the ISO images dated 20230223 (V12) and 20230227 (V11) or later are not vulnerable.