Security Advisory 2023-086

Critical Vulnerabilities in Veeam ONE

November 7, 2023 — v1.0

TLP:CLEAR

History:

- *07/11/2023 — v1.0 – Initial publication*

Summary

On November 6 2023, Veeam has released an advisory [1] addressing critical vulnerabilities affecting the Veeam ONE product. These vulnerabilities could allow an attacker to steal NTLM hashes, or to achieve Remote Code Execution.

Veeam has released hotfixes for these vulnerabilities, and it is recommended applying them as soon as possible.

Technical Details

- The vulnerability `CVE-2023-38548`, with a CVSS score of 9.8 out of 10, could allow an unprivileged user who has access to the Veeam ONE Web Client the ability to acquire the NTLM hash of the account used by the Veeam ONE Reporting Service.
- The vulnerability `CVE-2023-38547`, with a CVSS score of 9.9 out of 10, could allow an unauthenticated user to gain information about the SQL server connection Veeam ONE uses to access its configuration database. This may lead to remote code execution on the SQL server hosting the Veeam ONE configuration database.

Affected Products

- The vulnerability `CVE-2023-38547` affects Veeam ONE 11, 11a, 12.
- The vulnerability `CVE-2023-38548` Veeam ONE 12.

Versions outside of the support window (i.e., versions that have reached End-of-Life) may also be affected.

Recommendations

CERT-EU recommends applying the hotfixes as soon as possible by following Veeam guidance [1].

References

[1] https://www.veeam.com/kb4508