Security Advisory 2022-019

Multiple Critical Vulnerabilities in Veeam

March 21, 2022 — v1.0

TLP:WHITE

History:

- *21/03/2022 — v1.0 – Initial publication*

Summary

On 12/03/2022 Veeam has published multiple critical vulnerabilities (CVE-2022-26500, CVE-2022-26501) [2, 3] in Veeam products which allow remote code execution without authentication. This vulnerability may lead to gaining control over the targeted system. The publication was last modified by Veeam on 18/03/2022 [1].

Technical Details

The Veeam Distribution Service (TCP 9380 by default) allows unauthenticated users to access internal API functions. A remote attacker may send input to the internal API which may allow unauthenticated users to upload and execute malicious code on the affected products.

Affected Products

According to Veeam the affected products are:

- Veeam Backup & Replication 9.5
- Veeam Backup & Replication 10
- Veeam Backup & Replication 11

However, all new deployments of Veeam Backup & Replication version 11a and 10a installed using the ISO images dated 20220302 or later are not vulnerable [1].

Recommendations and Mitigations

CERT-EU recommends following the specific steps listed for each of the following version of the product:

Patches are available for the following product versions [1]:

- Veeam Backup & Replication 11a (build 11.0.1.1261 P20220302)
- Veeam Backup & Replication 10a (build 10.0.1.4854 P20220304)

There is no patch for the Veeam Backup & Replication 9.5, because the support of the product has ended on January 2022 [4]. Veeam suggests upgrading to supported versions of the product [5].

As a temporary mitigation of the vulnerabilities it is suggested by Veeam to stop and disable the Veeam Distribution Service. The Veeam Distribution Service is installed on the Veeam Backup & Replication server and servers specified as distribution servers in Protection Groups.

References

[1] https://www.veeam.com/kb4288

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26500

[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26501

[4] https://www.veeam.com/product-lifecycle.html

[5] https://helpcenter.veeam.com/docs/backup/vsphere/upgrade_vbr.html?ver=110