Multiple Critical Vulnerabilities in Veeam

14th March 2022

Ticket Number: EN250299

This advisory is sent out in part that stakeholders hold preventative management and precautions of their network.

Summary

Two critical vulnerabilities have been disclosed in Veeam Backup & Replication. CVE-2022-26500, which has a CVSS score of 9.8, allows a remote unauthenticated threat actor to access internal API functions which can then lead to execution of malicious code and uploading of malicious files. CVE-2022-26501, which has a CVSS score of 9.8, allows a remote unauthenticated threat actor to access internal API functions which can then lead to execution of malicious code and uploading of malicious files. The version which is affected by these vulnerabilities and is not supported by the issued updates is:

- Veeam Backup & Replication 9.5

CSIRTMalta encourages everyone to upgrade to Veeam Backup & Replication version 11 or 10 which is installed using ISO images dated 20220302 or later. As a temporary mitigation, entities can disable Veeam Distribution Service.

Additional Information and References:

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

CSIRTMalta Team

MINISTRY FOR HOME AFFAIRS
NATIONAL SECURITY AND LAW ENFORCEMENT