Security Advisory 2023-003

Critical Vulnerability in VMware vRealize Log Insight

January 26, 2023 — v1.0

TLP:CLEAR

History:

- *26/01/2023 — v1.0 – Initial publication*

Summary

On January 24, 2023, VMware released a new security advisory revealing multiple vulnerabilities in VMware vRealize Log Insight [1]. There are two critical vulnerabilities including a directory traversal vulnerability (`CVE-2022-31706`) and a broken access control vulnerability (`CVE-2022-31704`). Both of them have the CVSS score of 9.8 out of 10.

It is highly recommended applying the last version.

Technical Details

By exploiting these critical vulnerabilities, an unauthenticated actor can inject files into the operating system of an impacted appliance and could achieve remote code execution.

Affected Products

- VMware vRealize Log Insight 8.x
- VMware Cloud Foundation (VMware vRealize Log Insight) 4.x, 3.x

Recommendations

CERT-EU highly recommends applying the latest version or the workarounds provided by VMware [1].

References

[1] https://www.vmware.com/security/advisories/VMSA-2023-0001.html