Security Advisory 2022-076

Critical Vulnerability in VMware Cloud Foundation

October 31, 2022 — v1.0

TLP:CLEAR

History:

- *31/10/2022 — v1.0 – Initial publication*

Summary

On October 25, 2022, VMWare released a new version of Cloud Foundation (NSX-V) fixing a critical Remote Code Execution vulnerability [1]. VMware has confirmed that exploit code leveraging `CVE-2021-39144` against impacted products has been published [2]. It is highly recommended applying the last version.

Technical Details

The vulnerability, identified by `CVE-2021-39144`, with a CVSS score of 9.8 out of 10, is due to an unauthenticated endpoint that leverages XStream for input serialization in VMware Cloud Foundation (NSX-V). By exploiting this vulnerability, an unauthenticated attacker could achieve remote code execution in the context of the `root` user on the affected server.

Affected Products

- All versions for VMware NSX Data Center for vSphere (NSX-V) prior to NSX-V 6.4.14 appliances [3]
- All the VMware Cloud Foundation(VCF) 3.x versions

Recommendations

CERT-EU highly recommends applying the latest version or the workaround provided by VMWare.

References

[1] https://www.vmware.com/security/advisories/VMSA-2022-0027.html

[2] https://srcincite.io/blog/2022/10/25/eat-what-you-kill-pre-authenticated-rce-in-vmware-nsx-manager.html

[3] https://kb.vmware.com/s/article/89809