Security Advisory 2023-089

VMware Cloud Director Critical Vulnerability

November 20, 2023 — v1.0

TLP:CLEAR

History:

- *20/11/2023 — v1.0 – Initial publication*

Summary

On November 14, 2023, VMware issued an advisory about a critical authentication bypass vulnerability, `CVE-2023-34060`, affecting Cloud Director Appliance. The CVSSv3 score is 9.8, indicating a critical level of severity. This vulnerability is present on an upgraded version of VMware Cloud Director Appliance [1].

Technical Details

The vulnerability `CVE-2023-34060` allows a malicious actor with network access to bypass login restrictions when authenticating on port 22 (ssh) or port 5480 (appliance management console). This bypass is not present on port 443 (VCD provider and tenant login) or in new installations of VMware Cloud Director Appliance 10.5.

Affected Products

VMware Cloud Director Appliance (VCD Appliance) 10.5 if upgraded from 10.4.x or below.

Recommendations

It is recommended applying fixes as soon as possible [2].

Workaround

When it is not possible to update the last fixed version, one can apply the workaround published by VMWare [2].

References

[1] https://www.vmware.com/security/advisories/VMSA-2023-0026.html

[2] https://kb.vmware.com/s/article/95534