November 15, 2023

Overall rating: Critical

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that published a security advisory to address a vulnerability in the following product:

- VMware Cloud Director Appliance – version 10.5 if upgraded from 10.4.x or below.

Technical Details

On an upgraded version of VMware Cloud Director Appliance 10.5, a malicious actor with network access to the appliance can 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). On a new installation of VMware Cloud Director Appliance 10.5, the bypass is not present.

These vulnerabilities are rated as an overall **Critical** Severity.

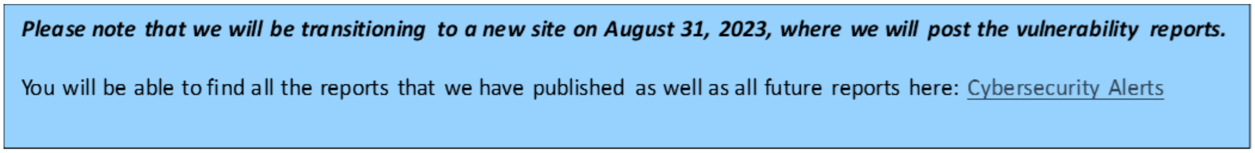
Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-34060
- VMware Security Advisory - VMSA-2023-0026
- VMware Security Advisories



Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts