October 25, 2023

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a VMware vulnerability. The vulnerability affects in the following products:

- VMware vCenter Server – multiple versions
- VMware Cloud Foundation (VMware vCenter Server) – versions 5.x and 4.x

Technical Details

vCenter Server contains an out-of-bounds write vulnerability in the implementation of the DCERPC protocol. VMware has evaluated the severity of this issue to be in the Critical severity range with a maximum CVSSv3 base score of 9.8.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

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

References

- CVE-2023-34048
- VMSA-2023-0023

- 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