

Overall rating: High



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

Summary

The Vulnerability and Risk Management (VRM) Team is aware VMware has published a Security Advisory to address vulnerabilities in the following products:

- VMware Cloud Foundation – multiple versions
- VMware vCenter Server – multiple versions

Technical Details

The vCenter Server contains a heap overflow vulnerability due to the usage of uninitialized memory in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may exploit this issue to execute arbitrary code on the underlying operating system that hosts vCenter Server.

These vulnerabilities are rated as an overall **High** 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

- [VMware Security Advisory - VMSA-2023-0014](#)
- [VMware Security Advisories](#)