November 15, 2023

Overall Rating - High

BRITISH COLUMBIA

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

Summary

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

- Citrix Hypervisor – version 2 CU1 LTSR

Technical Details

An issue has been discovered that affects Citrix Hypervisor 8.2 CU1 LTSR and may allow malicious privileged code in a guest VM to compromise an AMD-based host via a passed through PCI device (CVE-2023-46835).

In addition, Intel has disclosed a security issue affecting certain Intel CPUs (CVE-2023-23583). Although this is not an issue in the Citrix Hypervisor product itself, we have included updated Intel microcode to mitigate this CPU hardware issue. This issue may allow unprivileged code in a guest VM to compromise that VM and, potentially, the host.

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

- CVE-2023-23583, CVE-2023-46835
- Citrix Security Advisory - CTX583037
- Citrix 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