CERT-EU

Security Advisory 2023-091

High Vulnerabilities in Citrix Hypervisor

November 20, 2023 — v1.0

TLP:CLEAR

History:

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

Summary

On November 15, 2023, Citrix issued an advisory regarding two vulnerabilities affecting Citrix Hypervisor 8.2 CU1 LTSR that could allow malicious code in a guest VM to compromise the host [1].

Technical Details

The vulnerability `CVE-2023-46835` may allow privileged malicious code in a guest VM to compromise an AMD-based host via a passed through PCI device.

The vulnerability `CVE-2023-23583`, with a CVSS score of 8.8, affects the Intel 'Ice Lake' (2019) and later Intel processor generations. Although this is not an issue in the Citrix Hypervisor product itself, Citrix teams 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.

Affected Products

These vulnerabilities affect the Citrix Hypervisor 8.2 CU1 LTSR.

- CVE-2023-23583 only affects systems running on Intel Ice Lake or later CPUs.
- CVE-2023-46835 only affects systems that have both of a PCI device passed through to the guest VM by the host administrator and also an AMD CPU. Customers who are not using AMD CPUs and customers who are not using the PCI pass-through feature are not affected by this issue.

Recommendations

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

References

[1] https://support.citrix.com/article/CTX583037/citrix-hypervisor-security-bulletin-for-cve202323583-and-cve202346835

[2] https://support.citrix.com/article/CTX583402/hotfix-xs82ecu1057-for-citrix-hypervisor-82-cumulative-update-1