May 8, 2024

Overall rating: Medium

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware Citrix published a security advisory to address a vulnerability in the following product:

- XenCenter for Citrix Hypervisor – version 8.2 CU1 LTSR

Technical Details

Versions of XenCenter for Citrix Hypervisor 8.2 CU1 LTSR included a 3rd-party component, PuTTY, that is used to enable SSH connections from XenCenter to guest VMs when the "Open SSH Console" button is selected. The inclusion of PuTTY with XenCenter for Citrix Hypervisor 8.2 CU1 LTSR was deprecated with version 8.2.6 of XenCenter and any versions after 8.2.7 will not include PuTTY.

An issue has been reported in versions of PuTTY prior to version 0.81; when used in conjunction with XenCenter, this issue may, in some scenarios, allow an attacker who controls a guest VM to determine the SSH private key of a XenCenter administrator who uses that key to authenticate to that guest VM while using an SSH connection.

This issue has the following identifier:

- CVE-2024-31497

What Customers Should Do

Customers who do not wish to use the "Open SSH Console" functionality may remove the PuTTY component completely. Customers who wish to maintain the existing usage of PuTTY should replace the version installed on their XenCenter system with an updated version (with a version number of at least 0.81).

Note that versions of XenCenter for XenServer 8 have never included PuTTY.

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

This vulnerability is rated as a **MEDIUM** 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-2024-31497
- Citrix Security Advisory – CTX633416
- Citrix Security Advisories