

Overall Rating - High



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

Summary

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

- XenServer – version 8
- Citrix Hypervisor – version 8.2 CU1 LTSR

Exploitation of these vulnerabilities could allow information disclosure and denial of service.

Technical Details

A memory leak exists in Palo Alto Networks PAN-OS software that enables an attacker to send a burst of crafted packets through the firewall that eventually prevents the firewall from processing traffic. This issue applies only to PA-5400 Series devices that are running PAN-OS software with the SSL Forward Proxy feature enabled.

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-2023-46842 CVE-2024-2201 CVE-2024-31142
- [Citrix Security Advisory – CTX633151](#)
- [Citrix Security Advisories](#)