January 16, 2024

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 that Citrix published security advisories to address vulnerabilities in multiple products. Included were updates for the following:

- NetScaler ADC and NetScaler Gateway 14.1 — versions prior to 14.1-12.35
- NetScaler ADC and NetScaler Gateway 13.1 — versions prior to 13.1-51.15
- NetScaler ADC and NetScaler Gateway 13.0 — versions prior to 13.0-92.21
- NetScaler ADC 13.1-FIPS — versions prior to 13.1-37.176
- NetScaler ADC 12.1-FIPS — versions prior to 12.1-55.302
- NetScaler ADC 12.1-NDcPP — versions prior to 12.1-55.302

Technical Details

CVE- 2023- 6548 only impacts the management interface. Cloud Software Group strongly recommends that network traffic to the appliance's management interface is separated, either physically or logically, from normal network traffic. In addition, we recommend that you do not expose the management interface to the internet, as explained in the secure deployment guide. Removing such exposure to the internet greatly reduces the risk of exploitation of this issue. See NetScaler secure deployment guide (https://docs.citrix.com/en-us/citrix-adc/citrix-adc-secure-deployment/secure-deployment-guide.html) for more information.

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-2023-6548, CVE-2023-6549
- Citrix Security Advisory – CTX584986
- Citrix Security Advisories