July 9, 2024

Overall Rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a recently released Citrix security advisories to address vulnerabilities in the following products:

- Citrix Virtual Apps and Desktops – versions prior to 2402 Long Term Service Release (LTSR)
- Citrix Virtual Apps and Desktops – version 1912 LTSR prior to CU9
- Citrix Virtual Apps and Desktops – version 2203 LTSR prior to CU5
- NetScalar Console – multiple versions
- NetScalar SVM – multiple versions
- NetScalar Agent – multiple versions

Technical Details

Cloud Software Group strongly urges customers of NetScaler Console to install the relevant updated versions of NetScaler Console as soon as possible:

- NetScaler Console 14.1-25.53 and later releases of 14.1
- NetScaler Console 13.1-53.22 and later releases of 13.1
- NetScaler Console 13.0-92.31 and later releases of 13.0
- NetScaler SVM 14.1-25.53 and later releases of 14.1
- NetScaler SVM 13.1-53.17 and later releases of 13.1
- NetScaler SVM 13.0-92.31 and later releases of 13.0
- NetScaler Agent 14.1-25.53and later releases of 14.1
- NetScaler Agent 13.1-53.22 and later releases of 13.1
- NetScaler Agent 13.0-92.31and later releases of 13.0

This vulnerability is rated as a **CRITICAL** risk. Software updates exist to address these risks.

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 at vulnerabilityandriskmanagement@gov.bc.ca

References

- CVE-2024-6235 CVE-2024-6236 CVE-2024-6151
- Citrix Security Advisory – CTX677998
- Citrix Security Advisory – CTX678035
- Citrix Security Advisories