**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 Multiple vulnerabilities have been discovered in NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway).

The following supported versions of NetScaler ADC and NetScaler Gateway are affected by the vulnerabilities:

- NetScaler ADC and NetScaler Gateway 13.1 before 13.1-49.13
- NetScaler ADC and NetScaler Gateway 13.0 before 13.0-91.13
- NetScaler ADC 13.1-FIPS before 13.1-37.159
- NetScaler ADC 12.1-FIPS before 12.1-55.297
- NetScaler ADC 12.1-NDcPP before 12.1-55.297
- Note: NetScaler ADC and NetScaler Gateway version 12.1 is now End Of Life (EOL) and vulnerable.

This bulletin only applies to customer-managed NetScaler ADC and NetScaler Gateway. Customers using Citrix-managed cloud services or Citrix-managed Adaptive Authentication do not need to take any action.

## Technical Details

- **Reflected Cross-Site Scripting (XSS)** - CVE-2023-3466
  Requires victim to access an attacker-controlled link in the browser while being on a network with connectivity to the NSIP
- **Privilege Escalation to root administrator (nsroot) -** CVE-2023-3467
- **Unauthenticated remote code execution** - CVE-2023-3519
  Appliance must be configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) OR AAA virtual server

Exploits of CVE-2023-3519 on unmitigated appliances have been observed. Cloud Software Group strongly urges affected customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions as soon as possible.

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

- https://support.citrix.com/securitybulletins