SecurityRisk ADVISORS

Threat Bulletin

TB22-1213-Amber-Citrix

Executive Summary

On December 13, 2022, Citrix disclosed CVE-2022-27518, a CVSS 9.8 critical vulnerability impacting Citrix ADC and Citrix Gateway products. Citrix has confirmed the vulnerability is being exploited in attacks by state-sponsored adversaries.

Affected Products

The following customer-managed product versions are affected by this vulnerability. Products that are cloud-based services are not at risk.

- Citrix ADC and Citrix Gateway 13.0 before 13.0-58.32
- Citrix ADC and Citrix Gateway 12.1 before 12.1-65.25
- Citrix ADC 12.1-FIPS before 12.1-55.291
- Citrix ADC 12.1-NDcPP before 12.1-55.291

Safeguards/Recommendations

All customers using affected builds should update the products to the current 12.1 or 13.0 versions. All Citrix ADC and Citrix Gateway versions before 12.1 are end-of-life (EOL) and require upgrading. No workarounds are available for this vulnerability apart from disabling SAML authentication and upgrading to a current version. Review the NSA's APT5: Citrix ADC Threat Hunting Guidance.

References

- https://support.citrix.com/article/CTX474995/citrix-adc-and-citrix-gateway-security-bulletin-for-cve202227518
- https://media.defense.gov/2022/Dec/13/2003131586/-1/-1/0/CSA-APT5-CITRIXADC-V1.PDF
- https://www.citrix.com/blogs/2022/12/13/critical-security-update-now-available-for-citrix-adc-citrix-gateway/
- https://nvd.nist.gov/vuln/detail/CVE-2022-27518

Version History

Version 1. Initial Report

Contact Us

24x7 SOC Phone: 215.867.9051
Email: soc@sra.io
Website: https://sra.io

Vendor: Citrix

CVE-ID: CVE-2022-27518

Published: DEC 13, 2022

CVSS V3 Overall Score: 9.8

Criticality: Critical

Patch Availability: Yes

Vulnerability Type: Remote Code Execution

Exploitability Metrics

Attack Vector: Network

Attack Complexity: Low

Privileges Required: None

User Interaction: None

Impact Metrics

Scope: Unchanged

Confidentiality: High

Integrity: High

Availability: High

Confidence Metrics

Exploitability: Not Defined

Remediation Level: Not Defined

Report Confidence: Not Defined