Security Advisory 2022-078

Severe Vulnerabilities in Citrix Gateway and Citrix ADC

November 9, 2022 — v1.0

TLP:CLEAR

History:

- *09/11/2022 — v1.0 – Initial publication*

Summary

On November 8, 2022, Citrix released a Security Bulletin regarding three severe vulnerabilities affecting its Citrix Gateway and Citrix ADC products [1]. Under specific configurations, the three vulnerabilities can enable attackers to gain unauthorised access to the device, perform remote desktop takeover, or bypass the login brute force protection.

It is highly recommended installing the last security updates.

Technical Details

- The Vulnerability `CVE-2022-27510` is a Critical-severity authentication bypass using an alternate path or channel. This vulnerability is exploitable only if the device is configured as a VPN gateway.
- The Vulnerability `CVE-2022-27513` is due to insufficient verification of data authenticity that could allow an attacker to take remote desktop sessions over via phishing. The flaw only exists if the appliance is configured as VPN (Gateway), and the RDP proxy functionality is configured.
- The Vulnerability `CVE-2022-27516` could allow an attacker to bypass the login brute force protection mechanism. This vulnerability can only be exploited if the appliance is configured as VPN (Gateway) or AAA virtual server with *Max Login Attempts* configuration.

Affected Products

The following supported versions of Citrix ADC and Citrix Gateway are affected by these vulnerabilities:

- Citrix ADC and Citrix Gateway 13.1 before 13.1-33.47
- Citrix ADC and Citrix Gateway 13.0 before 13.0-88.12
- Citrix ADC and Citrix Gateway 12.1 before 12.1.65.21
- Citrix ADC 12.1-FIPS before 12.1-55.289
- Citrix ADC 12.1-NDcPP before 12.1-55.289

Customers using Citrix-managed cloud services do not need to take any action.

Recommendations

CERT-EU highly recommends installing the latest updated versions of Citrix ADC or Citrix Gateway as soon as possible.

References

[1] https://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve202227510-cve202227513-and-cve202227516