Security Advisory 2022-087

Critical Vulnerability in Citrix Gateway and Citrix ADC

December 13, 2022 — v1.0

TLP:CLEAR

History:

- *13/12/2022 — v1.0 – Initial publication*

Summary

On December 13, 2022, Citrix released a Security Bulletin regarding a critical vulnerability CVE-2022-27518 affecting its Citrix Gateway and Citrix ADC products [1]. If exploited, this vulnerability can enable an unauthenticated remote attacker to perform arbitrary code execution on the appliance.

According to NSA, the vulnerability is being exploited by APT5 group [2, 3]. APT5 is also known to have exploited Pulse Secure VPN vulnerabilities in 2021. It is then highly recommended to install the last security updates.

Technical Details

This zero day vulnerability `CVE-2022-27518` is due to improper control of a resource through its lifetime. This vulnerability is exploitable only if Citrix ADC or Citrix Gateway is configured as a SAML SP or a SAML IdP.

Affected Products

The following supported versions of Citrix ADC and Citrix Gateway are affected by this vulnerability:

- 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

Citrix ADC and Citrix Gateway version 13.1 is unaffected. Moreover for Citrix-managed cloud services or Citrix-managed Adaptive Authentication there is not need to take any action.

For identifying if Citrix ADC or Citrix Gateway is configured as a SAML SP or a SAML IdP, you need to inspect the `ns.conf` file for the following commands:

- `add authentication samlAction` - Appliance is configured as a SAML SP or,

- `add authentication samlIdPProfile` - Appliance is configured as a SAML IdP

If either of the commands are present in the `ns.conf` file and if the version is an affected version, then the appliance must be updated.

Recommendations

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

- Citrix ADC and Citrix Gateway 13.0-58.32 and later releases
- Citrix ADC and Citrix Gateway 12.1-65.25 and later releases of 12.1
- Citrix ADC 12.1-FIPS 12.1-55.291 and later releases of 12.1-FIPS
- Citrix ADC 12.1-NDcPP 12.1-55.291 and later releases of 12.1-NDcPP

Please note that Citrix ADC and Citrix Gateway versions prior to 12.1 are EOL and customers on those versions are recommended to upgrade to one of the supported versions.

Detection

Please consider using the NSA APT5: Citrix ADC Threat Hunting Guidance [3] to verify possible compromise.

References

[1] https://support.citrix.com/article/CTX474995/citrix-adc-and-citrix-gateway-security-bulletin-for-cve202227518

[2] https://www.bleepingcomputer.com/news/security/hackers-exploit-critical-citrix-adc-and-gateway-zero-day-patch-now/

[3] https://media.defense.gov/2022/Dec/13/2003131586/-1/-1/0/CSA-APT5-CITRIXADC-V1.PDF