Security Advisory 2023-050

Citrix NetScaler Critical Vulnerability

July 19, 2023 — v1.0

TLP:CLEAR

History:
- 19/07/2023 — v1.0 – Initial publication

Summary

On July 18, 2023, Citrix released a security bulletin regarding one critical vulnerability and two high severity vulnerabilities affecting Citrix NetScaler Application delivery controllers (ADCs) and Netscaler Gateway [1]. Citrix Netscaler ADC is a purpose-built networking appliance used to improve the performance, security, and resiliency of applications delivered over the web [2]. Citrix NetScaler Gateway consolidates remote access infrastructure to provide single sign-on across all applications whether in a data center, in a cloud, or if the apps are delivered as SaaS apps. It allows people to access any app, from any device, through a single URL [3].

Technical Details

**CVE-2023-3519** (CVSS score of 9.8): Unauthenticated remote code execution. **Exploits of CVE-2023-3519 on unmitigated appliances have been observed!** In order to exploit the vulnerability the appliance must be configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA virtual server [1].

**CVE-2023-3466** (CVSS score of 8.3): Reflected Cross-Site Scripting (XSS). The vulnerability can be exploited if a victim access an attacker-controlled link in the browser while being on a network with connectivity to the appliance [1].

**CVE-2023-3467** (CVSS score of 8.0): Privilege Escalation to root administrator (**nsroot**). Authenticated access to NSIP or SNIP with management interface access is required in order to leverage this flaw [1].

Affected Products

The following supported versions of NetScaler ADC and NetScaler Gateway are affected by the vulnerabilities [1]:
- 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 is vulnerable [1].

**Recommendations**

CERT-EU highly recommends installing the latest updated versions as soon as possible.

**References**

