aDvens

Security for the greater good

Newscast

Critical vulnerability in Citrix

2024-01-17 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

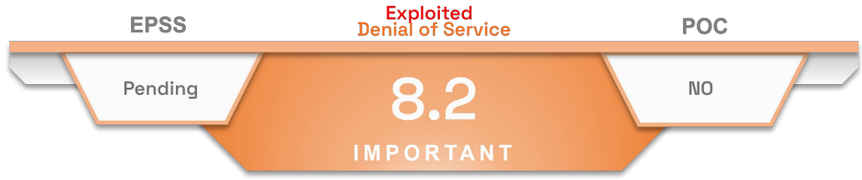
aDvens

Table of content

Citrix NetScaler - CVE-2023-6549 and CVE-2023-6548

On 16 January 2024, Citrix published an alert concerning two exploited zero-day in NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway).

CVE-2023-6549



This vulnerability allows a remote, unauthenticated attacker to cause a denial of service.

Few details about the vulnerability are currently available, but according to Citrix, in order to be vulnerable, NetScaler appliances must be configured as a Gateway (*VPN virtual server*, *ICA Proxy*, *CVPN*, *RDP Proxy*) or as an *AAA virtual server*.

This vulnerability is currently being exploited.

Type of vulnerability

- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

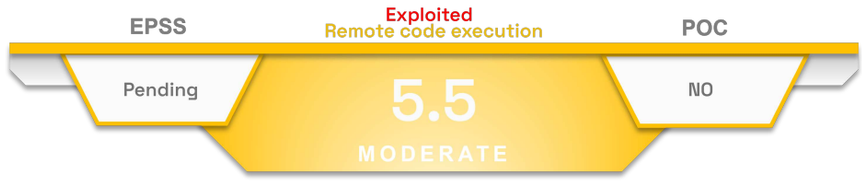
Risk

- Denial of Service

Severity (CVSS v3.1 base score)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	None
Privileges Required	None	Impact on integrity	Low
User Interaction	None	Impact on availability	High

CVE-2023-6548



This vulnerability allows an attacker, with network access to NetScaler's management interface, to execute arbitrary code on it.

This vulnerability is currently being exploited.

Type of vulnerability

- CWE-94: Improper Control of Generation of Code ('Code Injection')

Risk

- Remote code execution

Severity (CVSS v3.1 base score)

Attack vector	Adjacent	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	Low
Privileges Required	Low	Impact on integrity	Low
User Interaction	None	Impact on availability	Low

Impacted products

NetScaler ADC (formerly Citrix ADC) :

- Version 12.1 and prior
- Versions 12.1-NDcPP prior to 12.1-55.302
- Versions 12.1-FIPS prior to 12.1-55.302
- Versions 13.0 prior to 13.0-92.21
- Versions 13.1-FIPS prior to 13.1-37.176
- Versions 13.1 prior to 13.1-51.15
- Versions 14.1 prior to 14.1-12.35

NetScaler Gateway (formerly Citrix Gateway) :

- Version 12.1 and prior
- Versions 13.0 prior to 13.0-92.21
- Versions 13.1 prior to 13.1-51.15
- Versions 14.1 prior to 14.1-12.35

Recommendations

- Update NetScaler ADC to version 12.1-55.302, 13.0-92.21, 13.1-37.176, 13.1-51.15, 14.1-12.35 or later.
- Update NetScaler Gateway to version 13.0-92.21, 13.1-51.15, 14.1-12.35 or later.
- Additional information is available in Citrix's Advisory.

Proof of concept

No proof of concept is available in open source.

Sources

- https://www.cve.org/CVERecord?id=CVE-2023-6548
- https://www.cve.org/CVERecord?id=CVE-2023-6549
- https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549
- https://www.bleepingcomputer.com/news/security/citrix-warns-of-new-netscaler-zero-days-exploited-in-attacks/