CVE-2023-4966: Exploitation of Citrix NetScaler Information Disclosure Vulnerability

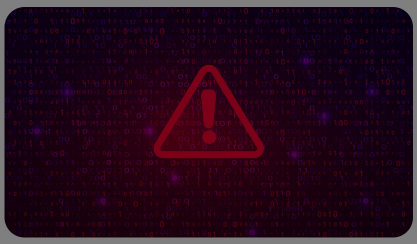
Oct 25, 2023 | 2 min read | Rapid7

Last updated at Fri, 27 Oct 2023 16:50:27 GMT

On October 10, 2023, Citrix published an advisory on two vulnerabilities affecting NetScaler ADC and NetScaler Gateway. The more critical of these two issues is CVE-2023-4966, a sensitive information disclosure vulnerability that allows an attacker to read large amounts of memory after the end of a buffer. Notably, that memory includes session tokens, which permits an attacker to impersonate another authenticated user. On October 17, Citrix updated the advisory to indicate that they have observed exploitation in the wild. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has also added CVE-2023-4966 to their Known Exploited Vulnerabilities (KEV) catalog.

On October 25, 2023, security firm Assetnote released an analysis, including a proof of concept, that demonstrates how to steal session tokens. Since then, Shadowserver has noted an uptick in scanning for that endpoint. Rapid7 MDR is investigating potential exploitation of this vulnerability in a customer environment but is not yet able to confirm with high confidence that CVE-2023-4966 was the initial access vector.

Rapid7 recommends taking emergency action to mitigate



Topics

- Metasploit (654)
- Vulnerability Management (359)
- Research (236)
- Detection and Response (205)
- Vulnerability Disclosure (148)
- Emergent Threat Response (141)
- Cloud Security (136)
- Security Operations (20)

Popular Tags

Search Tags

Metasploit
Metasploit Weekly Wrapup
Vulnerability Management
Research
Logentries
Detection and Response

Affected Products

Citrix published a blog on October 23 that has exploitation and mitigation details. Their advisory indicates that CVE-2023-4966 affects the following supported versions of NetScaler ADC and NetScaler Gateway:

* NetScaler ADC and NetScaler Gateway 14.1 before 14.1-8.50

* NetScaler ADC and NetScaler Gateway 13.1 before 13.1-49.15

* NetScaler ADC and NetScaler Gateway 13.0 before 13.0-92.19

* NetScaler ADC 13.1-FIPS before 13.1-37.164

* NetScaler ADC 12.1-FIPS before 12.1-55.300

* NetScaler ADC 12.1-NDcPP before 12.1-55.300

Note: NetScaler ADC and NetScaler Gateway version 12.1 is now End-of-Life (EOL) and is vulnerable.

In order to be exploitable, the appliance must be configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) OR AAA virtual server (which is a very common configuration). Citrix has indicated that customers using Citrix-managed cloud services or Citrix-managed Adaptive Authentication do not need to take any action.

Mitigation Guidance

Citrix NetScaler ADC and Gateway users should update to a fixed version immediately, without waiting for a typical patch cycle to occur. Additionally, Citrix's blog on CVE-2023-4966 recommends killing all active and persistent sessions using the following commands:

Multiple Vulnerabilities in Common Unix Printing System (CUPS) READ MORE

High-Risk Vulnerabilities in Common Enterprise Technologies READ MORE

CVE-2024-40766: Critical Improper Access Control Vulnerability Affecting SonicWall Devices READ MORE

```
clear lb persistentSessions
```

For more information, see Citrix's advisory.

Rapid7 Customers

InsightVM and Nexpose customers can assess their exposure to both of the CVEs in Citrix's advisory (CVE-2023-4966, CVE-2023-4967) with authenticated vulnerability checks available in the October 23 content release.

Download Rapid7's 2023 Mid-Year Threat Report ▶

POST TAGS

Emergent Threat Response

AUTHOR

Rapid7

SHARING IS CARING

VIEW RAPID7'S POSTS

Related Posts

EMERGENT THREA...

Fortinet FortiManager CVE-2024-47575 Exploited in Zero-Day

READ FULL POST

EMERGENT THREA...

Multiple Vulnerabilities in Common Unix Printing System

READ FULL POST

EMERGENT THREA...

High-Risk Vulnerabilities in Common Enterprise

READ FULL POST

EMERGENT THREA...

CVE-2024-40766: Critical Improper Access Control

READ FULL POST

VIEW ALL POSTS

RAPID7 PLATFORM PRODUCTS SERVICES RESOURCES COMPANY PARTNERS EN SIGN IN

Blog Vulnerability Management MDR Detection & Response Cloud Security App Security Metasploit All Topics START TRIAL

CUSTOMER SUPPORT

+1-866-390-8113 (Toll Free)

SALES SUPPORT

+1-866-772-7437 (Toll Free)

Need to report an Escalation or a Breach?

GET HELP

The Command Platform

Exposure Command

Managed Threat Complete

RESOURCES

Product Support

Resource Library

Our Customers

Events & Webcasts

Training & Certification

Cybersecurity Fundamentals

Vulnerability & Exploit Database

Company

Diversity, Equity, and Inclusion

Leadership

News & Press Releases

Public Policy

Open Source

Investors

Contact

Blog

Support Login

Careers