



Select ▾

START TRIAL


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

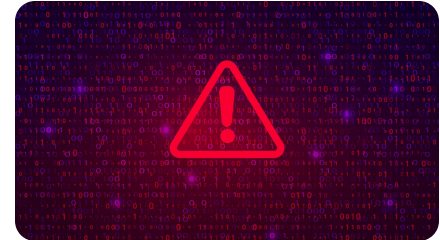
Oct 25, 2023 | 2 min read | [Rapid7](#)



*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



## Topics

Metasploit (653)

Vulnerability  
Management (359)

Research (236)

Detection and Response  
(205)

Vulnerability Disclosure  
(148)

Emergent Threat  
Response (141)

Cloud Security (136)


Security Operations (20)


## Popular Tags

Contact Us

Select ▾

START TRIAL

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

Metasploit

Metasploit Weekly  
Wrapup

Vulnerability  
Management

Research

Logentries

Detection and Response

## Related Posts


Fortinet  
FortiManager CVE-  
2024-47575  
Exploited in Zero-  
Day Attacks [READ](#)  
[MORE](#)

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

High-Risk  
Vulnerabilities in

Contact Us

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 CVE-2023-4966. Threat actors, including ransomware groups, have historically shown strong interest in Citrix NetScaler ADC vulnerabilities. We expect exploitation to increase. Our research team has [a technical assessment](#)  of the vulnerability and its impact in AttackerKB.

## Affected Products


CVE-2024-40700.  
Critical Improper  
Access Control  
Vulnerability  
Affecting SonicWall [READ](#)  
Devices [MORE](#)

Contact Us



Select ▾

START TRIAL

[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

Contact Us



Select ▾

START TRIAL

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

Contact Us



Select ▾

START TRIAL

```
kill lbaconnection -all
```

```
kill rdp connection -all
```

```
kill pcoipConnection -all
```

```
kill aaa session -all
```

```
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**



Contact Us

Emergent Threat Response

SHARING IS CARING



AUTHOR

Rapid7

VIEW RAPID7'S POSTS

## Related Posts

### EMERGENT THREAT RESPONSE

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

### EMERGENT THREAT RESPONSE

Multiple Vulnerabilities in Common Unix  
Printing System (CUPS)


Contact Us


**EMERGENT THREAT RESPONSE**  
High-Risk Vulnerabilities in Common Enterprise Technologies  
[READ FULL POST](#)


**EMERGENT THREAT RESPONSE**  
CVE-2024-40766: Critical Improper Access Control Vulnerability Affecting SonicWall Devices  
[READ FULL POST](#)

[VIEW ALL POSTS](#)









Select ▾

START TRIAL

Events & Webcasts

News & Press Releases


Training & Certification

Public Policy

Cybersecurity Fundamentals

Open Source

Vulnerability & Exploit Database


Investors 


CONNECT WITH US


Contact


Blog


Support Login

Careers 









© Rapid7

Legal Terms

Privacy Policy

Export Notice

Trust

Do Not Sell or Share My Personal Information

Cookie Preferences

Contact Us