

Citrix Bleed Attack

NetScaler ADC and NetScaler Gateway Vulnerability Actively Exploited

<https://www.netscaler.com/blog/news/cve-2023-4966-critical-security-update-now-available-for-netscaler-adc-and-netscaler-gateway/>
 CVEs: CVE-2023-4966

CVE-2023-4966 is being widely exploited, with multiple threat actors, including ransomware groups, targeting internet-accessible NetScaler ADC and Gateway instances. After exploiting CVE-2023-4966, the attackers may engage in network reconnaissance, stealing account credentials and moving laterally via RDP.

Background Citrix Netscaler is a network device providing load balancing, firewall and VPN services. NetScaler Gateway usually refers to the VPN and authentication components, whereas ADC refers to the load balancing and traffic management features. CVE-2023-4966 is a sensitive information disclosure vulnerability in NetScaler ADC and NetScaler Gateway .

As of October 30, Shadowserver spotted just over 5,000 vulnerable servers on the public internet.

Announced Oct. 10, 2023: Citrix released a security bulletin for a sensitive information disclosure vulnerability (CVE-2023-4966) impacting NetScaler ADC and NetScaler Gateway appliances.
<https://support.citrix.com/article/CTX579459/>

Oct 18, 2023: CISA added CVE-2023-4966 to its known exploited list, KEV catalog.

Oct 25, 2023 AssetNote researchers released a proof-of-concept (PoC) exploit demonstrating how to hijack a NetScaler account via session token theft.

Oct 31, 2023: Mandiant released campaign analysis targeting CVE-2023-4966
<https://www.mandiant.com/resources/blog/session-hijacking-citrix-cve-2023-4966>

Latest Developments Fortinet customers remain protected via the IPS signature "HTTP.Header.Overly.Long.Host.Field.Value" to detect and block any attack targeting the vulnerable Citrix servers and as of now, it has blocked attacks targeting the vulnerability on more than 5000 unique IPS devices.

FortiGuard also recommends to update and apply patches provided on the vendor advisory.
<https://www.netscaler.com/blog/news/cve-2023-4966-critical-security-update-now-available-for-netscaler-adc-and-netscaler-gateway/>


PROTECT


Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:


- Reconnaissance
- Weaponization
- Delivery
- Exploitation


IPS


Detects and blocks attack related to Citrix Bleed (CVE-2023-4966)


FortiGate
DB 14.524


FortiSASE
DB 14.524


FortiNDR
DB 14.524


FortiADC
DB 14.524



FortiProxy
DB 14.524


- Installation
- C2
- Action


DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:


Outbreak Detection

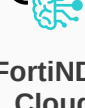

FortiAnalyzer
DB 2.00024


FortiSIEM
DB 601


FortiNDR Cloud

Threat Hunting


FortiAnalyzer
v6.4+



FortiNDR Cloud

RESPOND

Develop containment techniques to mitigate impacts of security events:


Automated Response


Services that can automatically respond to this outbreak.


FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.


Incident Response



FortiRecon: ACI


RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training


Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.


NSE Training


Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download and other forms of cyberattacks.



Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:


Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.


Security Rating

Business Reputation

Know attackers next move to protect against your business branding.


FortiRecon: EASM

Additional Resources

- Mandiant** <https://www.mandiant.com/resources/blog/session-hijacking-citrix-cve-2023-4966>
- The Register** https://www.theregister.com/2023/10/31/mass_exploitation_citrix_bleed/
- Shadow Server** https://dashboard.shadowserver.org/statistics/combined/time-series/?date_range=7&source=http_vulnerable&source=http_vulnerable6&tag=cve-2023-4966%2B&group_by=geo&style=stacked
- Bleeping Computer** <https://www.bleepingcomputer.com/news/security/hackers-use-citrix-bleed-flaw-in-attacks-on-govt-networks-worldwide/>
- Asset Note** <https://www.assetnote.io/resources/research/citrix-bleed-leaking-session-tokens-with-cve-2023-4966>

Learn more about [FortiGuard Outbreak Alerts](#)