Health-ISAC
Collaborating for Resilience in Health

THREAT BULLETINS

PoC Exploits Available for Citrix NetScaler ADC and NetScaler Gateway Flaw CVE-2025-5777

TLP:WHITE

Jul 09, 2025

Proof-of-Concept (PoC) exploits for a critical vulnerability, tracked as CVE-2025-5777 and dubbed CitrixBleed2, affecting Citrix NetScaler ADC and Gateway devices are publicly available.

Security researchers have confirmed that the security flaw's exploit complexity is low and can lead to the compromise of user session tokens. Successful exploitation allows threat actors to access memory contents by delivering specially crafted POST requests during login attempts.

Despite Citrix advising that there is no evidence to suggest CVE-2025-5777 is actively being exploited, security researchers have opposing information that indicates otherwise.

Given the criticality of CVE-2025-5777, readily available exploit code, and the ubiquity of Citrix NetScaler ADC and Gateway devices, Health-ISAC is sharing this information to increase situational awareness and encourage users to patch vulnerable instances immediately.

CVE-2025-5777 has a CVSS score of 9.3 and stems from an out-of-bounds memory read due to inadequate input validation. It impacts

systems configured as Gateway or Authentication, Authorization, and Accounting (AAA) servers.

Affected Versions:

- NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-43.56
- NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-58.32
- NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.235-FIPS and NDcPP
- NetScaler ADC 12.1-FIPS BEFORE 12.1-55.328-FIPS

While limited vendor-specific technical details hinder specific IoC recommendations, researchers from Horizon3.ai have identified several potential techniques to identify exploitation within systems:

Anomalous log entries:

- Look for non-printable characters in log entries, particularly if debug logging is enabled for login endpoints. These can indicate that session tokens might have been leaked.

Active session anomalies:

- Single-user sessions originating from multiple client IP addresses can indicate a compromise.
- Unusual or multiple active nsroot sessions.

Post-Exploitation Artifacts:

- Evidence of the creation of backdoor accounts, modification of running configurations to establish persistence, and the installation of remote access utilities.
- Evidence of any modifications to logging configurations.

Recommendations:

Health-ISAC recommends organizations review and assess their level of risk to this vulnerability and take the necessary actions to ensure risk mitigations are implemented, including:

- Immediately apply updates for the affected Citrix NetScaler ADC and Gateway devices.
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	horizon3, reliaquest, bleepingcomputer, infosecurity-magazine, cybersecuritynews, watchtowr, projectdiscovery, hhs

Alert ID f0ffd0b6

View Alert

Share Feedback

was this helpful? |

Tags CitrixBleed2, CVE-2025-5777, Citrix, NetScaler Gateway, NetScaler ADC

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**