Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Multiple Flaws in Citrix NetScaler ADC and Gateway Pose Immediate Threat

Date of Publication	Date of Publication	Admiralty Code	TA Number
June 27, 2025	September 2, 2025	A1	TA2025202

Summary

First Seen: June 2025
Affected Product: Citrix NetScaler ADC and NetScaler Gateway
Impact: Recent Citrix NetScaler vulnerabilities, including CVE-2025-6543 (memory overflow) and CVE-2025-5777 (CitrixBleed 2), pose critical risks like DoS, session hijacking, and MFA bypass. Both vulnerabilities are now being actively exploited in the wild. Affected versions include NetScaler ADC/Gateway prior to 14.1-47.46 and 13.1-59.19, as well as all EOL versions, including 12.1 and 13.0. Urgent patching and post-update session termination are strongly recommended.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-6543	Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✓	✓	✓
CVE-2025-5777	CitrixBleed 2 (Citrix NetScaler Gateway Out-of-Bounds Read Vulnerability)	Citrix NetScaler ADC and NetScaler Gateway	✗	✓	✓
CVE-2025-5349	Citrix NetScaler ADC and NetScaler Gateway Improper Access Control Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✗	✗	✓

Vulnerability Details

#1

Recently, critical vulnerabilities have been identified in NetScaler ADC and Gateway appliances, most notably CVE-2025-6543, a memory overflow flaw with a CVSS score of 9.2. This vulnerability has already been observed in active attacks, primarily resulting in denial of service but with the potential for more severe outcomes, such as unauthorized code execution. It affects appliances configured as VPNs, ICA proxies, CVPNs, RDP proxies, or AAA servers running versions prior to 14.1-47.46, 13.1-59.19, and all unsupported 12.1 and 13.0 releases.

#2

Another major issue, CVE-2025-5777 (dubbed “CitrixBleed 2”), is a critical out-of-bounds read vulnerability (CVSS 9.3) that could allow attackers to extract session tokens from memory. This enables session hijacking and bypass of multi-factor authentication, echoing the notorious 2023 CitrixBleed incident. This vulnerability is now being actively exploited in the wild, and publicly available proof-of-concept (PoC) exploit code has further accelerated the risk of widespread attacks.

#3

Citrix has also addressed CVE-2025-5349, a high-severity improper access control vulnerability in the management interface. Updated fixes for all three vulnerabilities are available in builds 14.1-47.46 and later, 13.1-59.19 and later, as well as their respective FIPS/NDcPP variants. Appliances running unsupported versions (12.1 and 13.0) remain exposed and should be upgraded or decommissioned immediately.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-6543	NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-47.46, 13.1 BEFORE 13.1-59.19 NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.236-FIPS and NDcPP	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:-:*:*:* cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:fips:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:ndcpp:*:*:*	CWE-119

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-5777	NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-43.56, 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	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:-:*:*:* cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:fips:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:ndcpp:*:*:*	CWE-125
CVE-2025-5349			CWE-284

Recommendations

Apply Security Updates Immediately: Organizations must prioritize patching all customer-managed Citrix NetScaler ADC and Gateway appliances to secure versions. The affected versions include 14.1 (before 14.1-47.46), 13.1 (before 13.1-59.19), and 13.1 FIPS/NDcPP (before 13.1-37.236). Appliances running 12.1 or 13.0 should be decommissioned, as these versions are End-of-Life and will not receive patches.

Terminate Active Sessions Post-Patch: After patching, proactively kill all active ICA and PCoIP sessions to invalidate potentially compromised session tokens:

- kill icaconnection –all
- kill pcoipConnection –all

This ensures that any existing session tokens potentially exposed prior to patching are invalidated.

Restrict Internet Exposure: Public-facing NetScaler appliances are the primary attack surface for this vulnerability. Wherever possible, restrict external access using VPNs, firewalls, or segmentation strategies. Limit access to management interfaces and authentication services (e.g., AAA virtual servers) to trusted IP ranges only.

Implement Defense-in-Depth Controls: Apply layered security measures to reduce risk even if exploitation occurs. This includes enforcing least privilege on all administrative interfaces, using strong authentication methods, and segregating NetScaler systems from high-value targets within the network. Log access to all NetScaler interfaces for audit and alerting purposes.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0042 Resource Development	TA0001 Initial Access	TA0040 Impact
TA0002 Execution	TA0004 Privilege Escalation	TA0006 Credential Access	TA0005 Defense Evasion
T1588.006 Vulnerabilities	T1068 Exploitation for Privilege Escalation	T1203 Exploitation for Client Execution	T1059 Command and Scripting Interpreter
T1556 Modify Authentication Process	T1190 Exploit Public-Facing Application	T1588 Obtain Capabilities	T1498 Network Denial of Service
T1552 Unsecured Credentials	T1588.005 Exploits	T1134 Access Token Manipulation	

Patch Links

https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694788

https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420

References

https://www.fortiguard.com/threat-signal-report/6134/citrix-netscaler-adc-and-netscaler-gateway-vulnerabilities

https://www.hivepro.com/threat-advisory/a-longstanding-zero-day-in-citrix-devices-exploited-since-august/

https://labs.watchtowr.com/how-much-more-must-we-bleed-citrix-netscaler-memory-disclosure-citrixbleed-2-cve-2025-5777/

http://horizon3.ai/attack-research/attack-blogs/cve-2025-5777-citrixbleed-2-write-up-maybe/

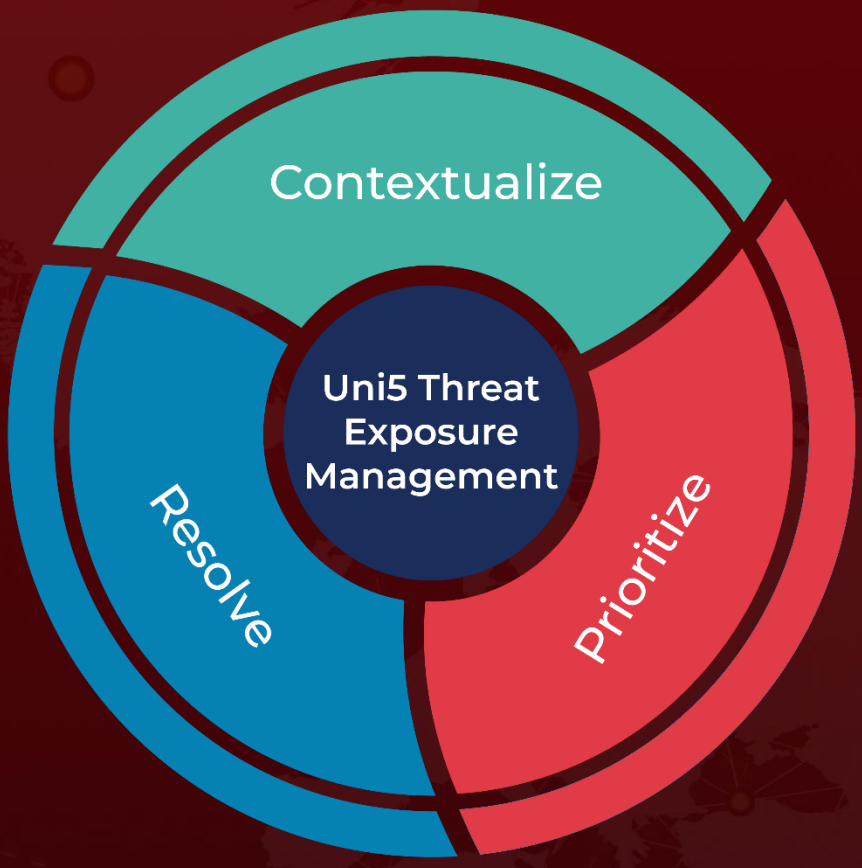
https://github.com/win3zz/CVE-2025-5777

https://www.netscaler.com/blog/news/netscaler-critical-security-updates-for-cve-2025-6543-and-cve-2025-5777/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

June 27, 2025 • 7:30 AM

More at www.hivepro.com