CYBER ADVISORY

TLP:CLEAR
25 June 2025

Citrix NetScaler ADC and NetScaler Gateway Critical Vulnerabilities

Citrix | NetScaler | Active Exploitation | Critical Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of two critical vulnerabilities impacting Citrix NetScaler ADC and NetScaler Gateway. CVE-2025-6543 has a CVSS v4.0 score of 9.2, the vulnerability is a memory overflow leading to unintended control flow and denial of service when NetScaler ADC and NetScaler Gateway are configured as a gateway or AAA virtual server.[1] Citrix has confirmed exploitation of CVE-2025-6543 on unmitigated appliances.[2] CVE-2025-5777 has a CVSS v4.0 score of 9.3, the vulnerability is an insufficient input validation leading to memory overread when NetScaler is configured as a gateway or AAA virtual server.[3] CVE-2025-5777 can be exploited remotely without authentication, allowing attackers to read session tokens or other sensitive information in memory.[4]

Affected Versions (CVE-2025-6543):

- NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-47.46
- NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-59.19
- NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.236-FIPS and NDcPP

Affected Versions (CVE-2025-5777):

- 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

The Cal-CSIC recommends immediately applying the mitigations provided by Citrix's security bulletins due to high probably of active exploitation.

Citrix Security Bulletin: CVE-2025-6543

Citrix Security Bulletin: CVE-2025-5777

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

[1] National Vulnerability Database; "CVE-2025-6543 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2025-6543; accessed 25 June 2025
[2] Citrix; "NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2025-6543"; https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694788; accessed 25 June 2025
[3] National Vulnerability Database; "CVE-2025-5777 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2025-5777; accessed 25 June 2025
[4] The Register; "Don't panic, but it's only a matter of time before critical 'CitrixBleed 2' is under attack"; https://www.theregister.com/2025/06/24/critical_citrix_bug_citrixbleed; accessed 25 June 2025