TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

Wednesday, August 27, 2025

CSIC-ADVISORY-202508-003

Citrix NetScaler ADC and NetScaler Gateway Critical Vulnerabilities

NetScaler ADC | Remote Code Execution | NetScaler Gateway | Memory Overflow

The California Cybersecurity Integration Center (Cal-CSIC) has identified three vulnerabilities affecting Citrix NetScaler Application Delivery Controller (ADC) and Gateway devices.

- CVE-2025-7775 (CVSS score: 9.2) - Memory overflow vulnerability leading to Remote Code Execution (RCE) and/or Denial-of-Service (DoS)[i]
- CVE-2025-7776 (CVSS score: 8.8) - Memory overflow vulnerability leading to unpredictable or erroneous behavior and DoS[ii]
- CVE-2025-8424 (CVSS score: 8.7) - Improper access control on the NetScaler Management Interface[iii]

The CSIC assesses that CVE-2025-7775 is the most critical, due to its active exploitation of unmitigated devices, and its capability to enable unauthenticated remote code execution. Successful exploitation allows an attacker to execute arbitrary code or cause a DoS condition on an affected device.[iv]

Affected Versions:

- NetScaler ADC and NetScaler Gateway 14.1 before 14.1-47.48
- NetScaler ADC and NetScaler Gateway 13.1 before 13.1-59.22
- NetScaler ADC 13.1-FIPS and NDcPP before 13.1-37.241-FIPS and NDcPP
- NetScaler ADC 12.1-FIPS and NDcPP before 12.1-55.330-FIPS and NDcPP

The Cal-CSIC recommends immediately applying the mitigations provided by Citrix security bulletin due to the severity of these vulnerabilities.

NetScaler ADC and NetScaler Gateway Security Bulletin

References

[i] National Vulnerability Database; “CVE-2025-7775 Detail” https://nvd.nist.gov/vuln/detail/CVE-2025-7775; accessed 26 August 2025

[ii] National Vulnerability Database; “CVE-2025-7776 Detail” https://nvd.nist.gov/vuln/detail/CVE-2025-7776; accessed 26 August 2025

[iii] National Vulnerability Database; “CVE-2025-8424 Detail” https://nvd.nist.gov/vuln/detail/CVE-2025-8424; accessed 26 August 2025

[iv] Tenable; “CVE-2025-7775: Citrix NetScaler ADC and NetScaler Gateway Zero-Day Remote Code Execution Vulnerability Exploited in the Wild” https://www.tenable.com/blog/cve-2025-7775-citrix-netscaler-adc-and-netscaler-gateway-zero-day-remote-code-execution; accessed 26 August 2025

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.