

06 OCT 2026



Active Exploitation of Citrix NetScaler SAML Memory Overflow Vulnerability

Unauthorized Access

Active Exploitation

Denial of Service

Fixed Releases Available

Executive Summary

The California Cybersecurity Integration Center (Cal-CSIC) has identified a high severity zero-day vulnerability under active exploitation, CVE-2026-88779, affecting Citrix NetScaler ADC and NetScaler Gateway deployments. CVE-2026-88779 is an improper restriction of operations within the bounds of a memory buffer vulnerability (CWE-119 / memory overflow) within NetScaler SAML authentication handling. An attacker operating remotely without valid credentials can trigger this vulnerability by sending malformed SAML authentication requests, crashing the authentication process or appliance to induce a sustained denial-of-service (DoS) condition. Exploitation requires no authentication, administrative credentials, or user interaction, but requires the appliance to be configured as a SAML Service Provider (SP) or SAML Identity Provider (IdP) bound to Gateway or AAA virtual servers¹. This vulnerability carries a CVSS v4.0 score of 8.7 (High)² and has been added to the CISA Known Exploited Vulnerabilities (KEV)³ catalog due to confirmed active exploitation.

Recommended Actions

The Cal-CSIC recommends the following actions from the [Citrix Advisory](#):

1. Audit Configurations for SAML Preconditions & Upgrade Deployments: Immediately identify devices configured with SAML authentication actions (samlAction) or SAML IdP profiles (samlIdPProfile) and upgrade them to the corresponding fixed NetScaler release (14.1-73.41, 13.1-64.28, 14.1-73.41 FIPS, or 13.1-37.282).
2. Apply Interim Virtual Patching via NetScaler Console:

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.

If immediate patching cannot be completed, enable the Global Deny List signature mitigation with virtual patching enabled via NetScaler Console to block exploit patterns from known malicious sources while scheduling emergency maintenance.

Affected Releases and Updated Version

Affected Version	Affected Range	Updated Version
NetScaler ADC / Gateway 14.1	Earlier than 14.1-73.41	Upgrade to 14.1-73.41 or later
NetScaler ADC / Gateway 13.1	Earlier than 13.1-64.28	Upgrade to 13.1-64.28 or later
NetScaler ADC 14.1-FIPS	Earlier than 14.1-73.41 FIPS	Upgrade to 14.1-73.41 FIPS or later
NetScaler ADC 13.1-FIPS / NDcPP	Earlier than 13.1-37.282	Upgrade to 13.1-37.282 or later

Sharing, Reporting, and Support

Sharing, Reporting, and Support

Sharing information and intelligence to state, local, federal, and private partners will ensure organizations across California can be better informed and defended.

For questions, concerns, or support or are interested in sharing information or intelligence in any cyber related matter, contact the Cal-CSIC via:

 833-REPORT-1 or 916.636.2997
 calcsic@caloes.ca.gov

Report suspicious or suspected foreign activity and incidents to:



Federal Officials at CISA and/or the FBI as applicable



Coordinate with your regional Fusion Center



information, intelligence, and IOCs with ISACs

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.

References:

¹ Citrix; " Understanding and Addressing CVE-2026-88779 in Citrix NetScaler ADC and Citrix NetScaler Gateway"; https://community.citrix.com/techzone-blogs/110_security-updates/understanding-and-addressing-cve-2026-88779-in-citrix-netscaler-adc-and-citrix-netscaler-gateway/; accessed 06 October 2026

² NIST; "CVE-2026-88779 Detail"; <https://nvd.nist.gov/vuln/detail/cve-2026-88779/>; /; accessed 06 October 2026

³ CISA; "Known Exploited Vulnerabilities Catalog"; https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-88779; accessed 06 October 2026

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.