



CYBER ADVISORY

Monday, September 28, 2026

CAL-CSIC-202609-A-013

Two Zero-Day Vulnerabilities Impacting Citrix NetScaler ADC and Citrix NetScaler Gateway

Zero-day Vulnerabilities

Internal Pivoting

Remote Code Execution

Patches Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of two actively exploited zero-day vulnerabilities impacting Citrix NetScaler ADC and Gateway. Both CVE-2026-88771 and CVE-2026-88772 carry a CVSS 4.0 score of 9.5.^{1,2} NetScaler Application Delivery Controller ensures the delivery of applications and services across the network, while Citrix NetScaler Gateway is primarily used for secure remote access to client resources via VPN, Web access, or Clientless access (via Citrix Gateway plug-in).

CVE-2026-88771 is an improper input validation within Citrix NetScaler ADC and Gateway which allows an unauthenticated attacker to construct malicious input that bypasses security checks and executes remote arbitrary commands on the underlying host. Successful exploitation gives the attacker control of the appliance to exfiltrate data, modify configurations, and pivot internally to other target resources.³

CVE-2026-88772 is a memory overflow vulnerability that can allow an attacker to execute arbitrary code or crash the targeted system. The vulnerability stems from improper bounds checking during the processing of incoming data that results in a buffer overflow. Successful exploitation allows the attacker to remotely take control of the targeted device/application or cause a Denial-of-Service.⁴

Citrix has issued a security bulletin not only for these two vulnerabilities, but also for six other medium-to-critical rated vulnerabilities. However, it is important to note that the two CVEs above are the ones out of the group considered to be zero-days and are under active exploitation.^{5,6} Citrix has issued patches to mitigate these vulnerabilities and have urged clients to install the relevant updates as soon as possible.

The Cal-CSIC recommends going to the security bulletin to see if you are affected by any of these vulnerabilities, and following Citrix's mitigation guidance and installing the relevant patches as soon as possible.

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.

For additional details regarding both CVEs, please use this link:

Citrix Security Bulletin: [CITRIX | Support](#)

Affected Products and Versions

Product	Affected Version	Patched Version
Citrix NetScaler ADC	< 14.1-73.37	14.1.73.37 and later
	< 13.1.64.23	13.1.64.23 and later
	< 14.1-73.37 FIPS	14.1-73.37 FIPS and later
	< 13.1.37.279 FIPS and NDcPP	13.1.37.279 FIPS and NDcPP and later
Citrix NetScaler Gateway	< 14.1-73.37	14.1.73.37 and later
	< 13.1-64.23	13.1.64.23 and later

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: [California Cybersecurity Integration Center | California Governor's Office of Emergency Services](#)

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.

TLP: CLEAR

References

¹ OpenCVE; "CVE-2026-88771"; <https://app.opencve.io/cve/CVE-2026-88771>; accessed 28 September 2026

² OpenCVE; "CVE-2026-88772"; <https://app.opecve.io/cve/CVE-2026-88772>; accessed 28 September 2026

³ Citrix; "Citrix NetScaler ADC and Citrix NetScaler Gateway Security Bulletin"; https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096&articleTitle=Citrix_NetScaler_ADC_and_Citrix_NetScaler_Gateway_Security_Bulletin_for_CVE_2026_88771_CVE_2026_88772_CVE_2026_88773_CVE_2026_88774_CVE_2026_88775_CVE_2026_88776_CVE_2026_88777_and_CVE_2026_88778; accessed 28 September 28, 2026

⁴ Citrix; "Citrix NetScaler ADC and Citrix NetScaler Gateway Security Bulletin"; https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096&articleTitle=Citrix_NetScaler_ADC_and_Citrix_NetScaler_Gateway_Security_Bulletin_for_CVE_2026_88771_CVE_2026_88772_CVE_2026_88773_CVE_2026_88774_CVE_2026_88775_CVE_2026_88776_CVE_2026_88777_and_CVE_2026_88778; accessed 28 September 28, 2026

⁵ CISA; Known Exploited Vulnerabilities Catalog; https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-88771; accessed 28 September 2026

⁶ CISA; Known Exploited Vulnerabilities Catalog; https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-88772; accessed 28 September 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.

TLP: CLEAR