# EXPLOITED VULNERABILITY ADVISORY: CVE-2026-8452

## Summary

CVE-2026-8452 in Citrix NetScaler ADC and NetScaler Gateway is being actively exploited in the wild. Memory overflow vulnerability NetScaler ADC and NetScaler Gateway leading to unpredictable or erroneous behavior and Denial of Service if the appliance is configured as a Gateway (SSL VPN, ICA Proxy, CVPN, RDP Proxy) or AAA virtual server CISA requires federal remediation by 2026-08-29; under the CRA, exploitation of an affected product must be reported within 24 hours.

## What we know

- **CVE:** CVE-2026-8452
- **Affected:** Citrix NetScaler ADC and NetScaler Gateway
- **Exploitation:** Actively exploited, added to CISA KEV on 2026-08-26
- **Severity:** CVSS 9.8 Critical, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
- **Exploitation likelihood (EPSS):** 2%
- **Weakness:** CWE-119

## Recommended action

Patch CVE-2026-8452 by 2026-08-29. If you cannot patch immediately, restrict network access to the affected service now (segment it, put it behind a VPN, or take it offline) until you can patch. If you ship an affected product, be ready to file the CRA 24-hour report the moment you find it exploited.

---

*Sources: CISA Known Exploited Vulnerabilities, NIST NVD. Public data; an advisory of active exploitation, not an incident report. Verify applicability to your estate before acting.*