Exploitation of vulnerabilities affecting Citrix NetScaler ADC and Citrix NetScaler Gateway

The NCSC is urging UK organisations to promptly mitigate vulnerabilities affecting Citrix NetScaler ADC and Gateway, two of which are being actively exploited.

What has happened?

Citrix has published a security bulletin detailing eight vulnerabilities affecting Citrix NetScaler ADC and Citrix NetScaler Gateway. Two of these, CVE-2026-88771 and CVE-2026-88772, have been confirmed as being **actively exploited**.

The NCSC is working to understand the impact of these vulnerabilities on UK organisations.

- **CVE-2026-88771:** Improper input validation allowing an unauthenticated remote attacker to execute arbitrary commands.
- **CVE-2026-88772:** Improper restriction of operations within the bounds of a memory buffer, leading to remote code execution or denial of service.
- **CVE-2026-88773:** Inconsistent interpretation of HTTP requests (HTTP request/response smuggling), which may allow an attacker to manipulate or bypass security controls.
- **CVE-2026-88774:** Improper HTTP URL-based expression usage leading to a feature policy bypass.
- **CVE-2026-88775:** Memory overflow vulnerability that may result in unpredictable or erroneous behaviour, or denial of service.
- **CVE-2026-88776:** Memory overflow vulnerability that may result in unpredictable or erroneous behaviour, or denial of service.
- **CVE-2026-88777:** Memory overflow vulnerability that may result in unpredictable or erroneous behaviour, or denial of service.
- **CVE-2026-88778:** Predictable exact value vulnerability that may allow an attacker to influence integrity or availability.

Who is affected?

Organisations using Citrix NetScaler ADC or Citrix NetScaler Gateway on premises are affected. The following supported versions of customer-managed Citrix NetScaler ADC and Citrix NetScaler Gateway are affected by the vulnerabilities:

- Citrix NetScaler ADC and Citrix NetScaler Gateway 14.1 before 14.1-73.37
- Citrix NetScaler ADC and Citrix NetScaler Gateway 13.1 before 13.1-64.23
- Citrix NetScaler ADC FIPS before 14.1-73.37 FIPS
- Citrix NetScaler ADC FIPS and NDcPP before 13.1-37.279

What should I do?

The NCSC recommends following vendor best practice advice to mitigate vulnerabilities.

The NCSC strongly urges network defenders to follow these priority actions:

1. Read the Citrix security bulletin and accompanying blog (includes IoCs) in full to determine if you have an affected system.
2. If possible, isolate the affected system(s) and replace with a new, fully up-to-date system (note this may cause service outage). For example, temporarily disable access to the service with upstream firewalls, disable the vulnerable

component(s) or restrict access to only the organisation's IP range.

3. Fully investigate for evidence of compromise using the published IoCs.
4. If you believe you have been compromised, and are in the UK, you should report it. You can also report the compromise to the vendor to assist their investigation.
5. Install the latest available updates (see Citrix blog for more details).
6. Re-enable/reintroduce the affected system(s).
7. Continue to monitor the Citrix security bulletin and perform continuous threat hunting activities. Customers can also use NetScaler Console File Integrity Monitoring to help detect unauthorised or unexpected changes to monitored files on managed NetScaler instances.

NCSC resources to help secure systems:

- Follow NCSC guidance including vulnerability management and preventing lateral movement.
- If your organisation is in the UK, you can sign up to the free NCSC Early Warning service to receive notifications of potential cyber threats on your network. If you are already an Early Warning user, please check your MyNCSC portal.
- The NCSC Vulnerability Disclosure Toolkit helps organisations of all sizes with the essential components of implementing a vulnerability disclosure process.

PUBLISHED

28 September 2026

NEWS TYPE

Alert