

# CVE-2023-3519

## Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability

Exigent

CISA KEV since Jul 19, 2023

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

Unauthenticated remote code execution

|                                              |                                           |                                                    |                                                                            |
|----------------------------------------------|-------------------------------------------|----------------------------------------------------|----------------------------------------------------------------------------|
| EVRS<br><b>94</b> /100<br>Immediate priority | CVSS V3.1<br><b>9.8</b><br>Critical · NVD | EPSS<br><b>0.997</b><br>99.95th percentile · FIRST | CISA DEADLINE<br><b>Aug 9, 2023</b><br>KEV since 2023 · listed over a year |
|----------------------------------------------|-------------------------------------------|----------------------------------------------------|----------------------------------------------------------------------------|

### Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

|                                                       |                            |                                                                |                                            |
|-------------------------------------------------------|----------------------------|----------------------------------------------------------------|--------------------------------------------|
| <input checked="" type="checkbox"/> <b>CISA KEV</b>   | Listed in the catalog      | <input type="checkbox"/> <b>Vendor exploitation</b>            | Confirmed exploitation in the wild         |
| <input checked="" type="checkbox"/> <b>Ransomware</b> | Known ransomware campaigns | <input type="checkbox"/> <b>KEV recency</b>                    | On the CISA KEV catalog for over two years |
| <input checked="" type="checkbox"/> <b>EPSS</b>       | 0.997 probability          | <input type="checkbox"/> <b>Pre-patch disclosure</b>           | Disclosure status unavailable              |
| <input checked="" type="checkbox"/> <b>CVSS</b>       | Base score 9.8             | <input type="checkbox"/> <b>Microsoft Exploitability Index</b> | Not a Microsoft CVE                        |

### Remediation

**Out-of-band / urgent** Patch or fixed version identified**CISA required action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

### Affected and fixed versions

| PACKAGE                                   | AFFECTED                                                                                   | FIXED IN                                               | SOURCE |
|-------------------------------------------|--------------------------------------------------------------------------------------------|--------------------------------------------------------|--------|
| netScaler application delivery controller | ≥ 12.1 < 12.1-55.297<br>≥ 13.0 < 13.0-91.13<br>≥ 13.1 < 13.1-37.159<br>≥ 13.1 < 13.1-49.13 | 12.1-55.297 · 13.0-91.13 ·<br>13.1-37.159 · 13.1-49.13 | NVD    |
| netScaler gateway                         | ≥ 13.0 < 13.0-91.13<br>≥ 13.1 < 13.1-49.13                                                 | 13.0-91.13 · 13.1-49.13                                | NVD    |

### Sources

**Vendor guidance** [github.com/advisories/GHSA-m4j4-rmj5-w5gp](https://github.com/advisories/GHSA-m4j4-rmj5-w5gp)**Additional guidance** [support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467](https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467)**NVD** [nvd.nist.gov/vuln/detail/CVE-2023-3519](https://nvd.nist.gov/vuln/detail/CVE-2023-3519)**CISA KEV** [cisa.gov/known-exploited-vulnerabilities-catalog](https://cisa.gov/known-exploited-vulnerabilities-catalog)**ENISA EUVD** [euvd.enisa.europa.eu/vulnerability/EUVD-2023-44176](https://euvd.enisa.europa.eu/vulnerability/EUVD-2023-44176)**Current data** [evulnable.com/vulnerability-management/cve/CVE-2023-3519](https://evulnable.com/vulnerability-management/cve/CVE-2023-3519)

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.