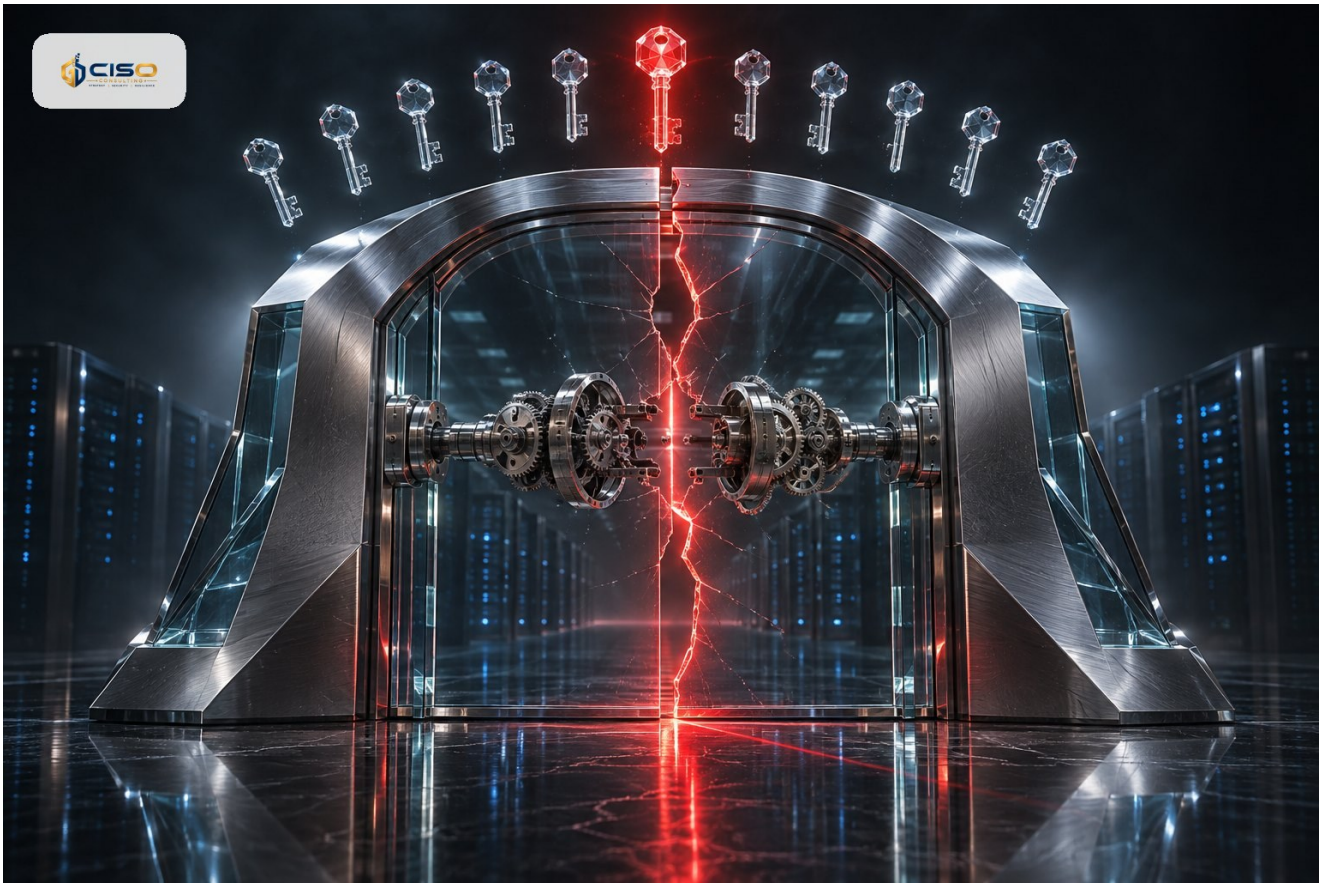
Citrix Patches 12 NetScaler and Secure Access Client Flaws, Including Authentication Bypass



Citrix has released patches for critical flaws in NetScaler ADC, NetScaler Gateway and NetScaler Console that could cause denial of service or authentication bypass. One listed flaw, CVE-2026-120868, scores 9.3 on CVSS.

- Affected products named in the source: NetScaler ADC, NetScaler Gateway and NetScaler Console.
- Possible impacts are denial of service (DoS) or authentication bypass.
- CVE-2026-120868 is a memory overflow flaw with a CVSS score of 9.3.
- The headline refers to 12 flaws across NetScaler and Secure Access Client.
- The source excerpt does not give affected versions or exploitation status.

Citrix has published patches for a set of security flaws affecting NetScaler ADC, NetScaler Gateway and NetScaler Console. According to the report, the most serious issues could lead to denial of service (DoS) or to an authentication bypass. The report's headline puts the total at 12 flaws across NetScaler and the Secure Access Client.

What is known

The one flaw detailed in the available text is **CVE-2026-120868**, a memory overflow vulnerability with a CVSS score of 9.3, affecting NetScaler ADC and NetScaler Gateway. The source describes the affected component only in part, and the remaining CVE entries are not included in the excerpt.

The excerpt does not state which versions are affected, which fixed builds to install, or whether any of the flaws are being exploited. Those details should be taken directly from Citrix's own security bulletin.

Why it matters

NetScaler ADC and Gateway commonly sit at the network edge and handle remote access and application delivery. An authentication bypass or a service outage on such devices can affect both security and availability, so institutions that run them should treat the update as a priority and confirm their exposure.

A calm, structured response is enough: identify the devices, read the vendor bulletin, and schedule the fixes through normal emergency change control.

What to do now

1. Inventory all NetScaler ADC, Gateway and Console instances, including Secure Access Client deployments.
2. Read Citrix's security bulletin to confirm affected versions and fixed builds for each CVE, including CVE-2026-120868.
3. Schedule patching of internet-facing NetScaler devices first under emergency change control.
4. Review authentication and access logs on NetScaler devices for unusual activity.
5. Record the exposure assessment and patch status for ECC and SAMA CSF evidence.