

## Security Advisory 2024-010

# Vulnerabilities in Netscaler ADS and Netscaler Gateway

July 18, 2024 — v1.1

TLP:CLEAR

### History:

- 17/01/2024 — v1.0 – Initial publication
- 18/07/2024 — v1.1 – Initial publication

### Summary

On January 16, 2024, Citrix released a security advisory addressing two vulnerabilities in Citrix NetScaler ADC and NetScaler Gateway, specifically [CVE-2023-6548](#) and [CVE-2023-6549](#). These vulnerabilities have been actively exploited and require urgent patching [1, 2].

[New] On July 17, The NHS England National Cyber Security Operations Centre announced that new intelligence provided by CrowdStrike indicates that contrary to Citrix's initial disclosure, the vulnerability [CVE-2023-6548](#) does not require user privileges for exploitation [3].

### Technical Details

[Updated] The vulnerability [CVE-2023-6548](#), with a CVSS score of 8.8, is an Unauthenticated Remote Code Execution (RCE) vulnerability in the NetScaler ADC and Gateway appliances. It can be exploited by an unauthenticated attacker with access to the appliance's management interface.

The vulnerability [CVE-2023-6549](#), with a CVSS score of 8.2, is a Denial of Service (DoS) vulnerability in the same appliances. It can be exploited when a vulnerable appliance has been configured as a Gateway (i.e., VPN, ICA Proxy, CVPN, RDP Proxy) or as an AAA virtual server.

### Affected Products

The vulnerabilities affect:

- NetScaler ADC and NetScaler Gateway 13.0 before 13.0-92.21;
- NetScaler ADC and NetScaler Gateway 13.1 before 13.1-51.15;
- NetScaler ADC and NetScaler Gateway 14.1 before 14.1-12.35;
- NetScaler ADC 12.1-NDcPP before 12.1-55.302;
- NetScaler ADC 12.1-FIPS before 12.1-55.302;
- NetScaler ADC 13.1-FIPS before 13.1-37.176.

## Recommendations

CERT-EU strongly recommends installing the releases patches for these vulnerabilities. Moreover, the vulnerability `CVE-2023-6548` only impacts the management interface, and, as recommended in the secure deployment guide of Citrix, this interface should not be exposed to the internet.

## References

- [1] <https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549>
- [2] <https://www.bleepingcomputer.com/news/security/citrix-warns-of-new-netscaler-zero-days-exploited-in-attacks/>
- [3] <https://digital.nhs.uk/cyber-alerts/2024/cc-4525>