National Cyber Security Centre

2310110140-NCSC

**Department of the Environment, Climate & Communications**

# NCSC Alert

## Critical and high severity vulnerabilities in NetScaler ADC and NetScaler Gateway - CVE-2023-4966, CVE-2023-4967 - Update

Wednesday 22nd November, 2023

**STATUS:** TLP-CLEAR

*Recipients can spread this to the world, there is no limit on disclosure. Sources may use* TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

# Revision History

| Revision | Date | Author(s) | Description |
|---|---|---|---|
| 1.0 | 11th October 2023 | CSIRT-IE | Initial advisory responding to Progress advisory |
| 1.1 | 2nd November 2023 | CSIRT-IE | Update with details of POC, exploitation and investigation details for CVE-2023-4966. |
| 1.2 | 22nd November 2023 | CSIRT-IE | Update with CISA details of exploitation of CVE-2023-4966. |

## Description

One critical and one high severity vulnerability have been discovered in customer managed NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway) devices which are being tracked as CVE-2023-4966 and CVE-2023-4967 respectively. Customers using Citrix-managed cloud services or Citrix-managed Adaptive Authentication do not need to take any action.

These are both unauthenticated buffer-related vulnerabilities affecting NetScaler ADC and NetScaler Gateway.

Citrix has released a security bulletin that addresses the vulnerabilities:

https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967.

### CVE-2023-4966 - 'Citrix Bleed'

Netscaler has since released an additional advisory with recommended next steps for customers affected by CVE-2023-4966.

The NCSC is aware of active exploitation in the wild along with details of a POC for the vulnerability. Security researchers at Mandiant have identified exploitation of CVE-2023-4966 at professional services, technology, and government organisations dating back to late August 2023.

## Products Affected

The following supported versions of NetScaler ADC and NetScaler Gateway are affected:

- NetScaler ADC and NetScaler Gateway 14.1 before 14.1-8.50
- NetScaler ADC and NetScaler Gateway 13.1 before 13.1-49.15
- NetScaler ADC and NetScaler Gateway 13.0 before 13.0-92.19
- NetScaler ADC 13.1-FIPS before 13.1-37.164
- NetScaler ADC 12.1-FIPS before 12.1-55.300
- NetScaler ADC 12.1-NDcPP before 12.1-55.300

Only devices configured as either a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) OR AAA virtual server are vulnerable to exploitation using these vulnerabilities.

## Impact

Exploitation of CVE-2023-4966 (CVSS 9.4) could allow the disclosure of sensitive information from vulnerable devices.

Exploitation of CVE-2023-4967 (CVSS 8.2) can potentially cause denial of service on vulnerable devices.

## Recommendations

The NCSC strongly advises affected organisations to identify any vulnerable devices and upgrade to one of the supported versions provided by Citrix that will address these vulnerabilities. Affected organisations should also initiate their incident response processes to ascertain if they have been compromised.

Further information can be found in Cisco's and Netscaler's security bulletins below:

https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967.

https://www.netscaler.com/blog/news/cve-2023-4966-critical-security-update-now-available-for-netscaler-adc-and-netscaler-gateway/.

Mandiant has released details of its investigation into CVE-2023-4966, including a YARA rule which may assist affected organisations in their own investigations. This can be accessed here:

https://www.mandiant.com/resources/blog/session-hijacking-citrix-cve-2023-4966

CISA has released detailed information on the exploitation of CVE-2023-4966 which is contained in the following two documents:

https://www.cisa.gov/sites/default/files/2023-11/MAR-10478915.r1.v1.CLEAR_.pdf

https://www.cisa.gov/sites/default/files/2023-11/AA23-325A%20LockBit%203.0%20Ransomware%20Affiliates%20Exploit%20CVE%202023-4966%20Citrix%20Bleed%20Vulnerability.pdf

**DISCLAIMER:** This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
**Tel:** +353 (0)1 6782333
**Mail:** certreport@decc.gov.ie
**Web:** ncsc.gov.ie
**Twitter:** ncsc_gov_ie
**LinkedIn:** ncsc-ie