National Cyber Security Centre

2307180130-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical and High severity vulnerabilities in NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway)

Tuesday 18th July, 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.

Description

One critical and two high severity vulnerabilities have been discovered in customer managed NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway) appliances which are being tracked as CVE-2023-3519, CVE-2023-3466 and CVE-2023-3467 respectively.

Cisco have reported that exploits of CVE-2023-3519 have been observed in the wild. This is a critical vulnerability with a CVSS of 9.8, if exploited, could allow an unauthenticated remote attacker to perform unauthenticated remote code execution on the appliance.

Citrix has released a security bulletin that addresses the vulnerabilities: https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467.

Products Affected

The following supported versions are affected:

- NetScaler ADC and NetScaler Gateway 13.1 before 13.1-49.13
- NetScaler ADC and NetScaler Gateway 13.0 before 13.0-91.13
- NetScaler ADC 13.1-FIPS before 13.1-37.159
- NetScaler ADC 12.1-FIPS before 12.1-65.36
- NetScaler ADC 12.1-NDcPP before 12.65.36

NetScaler ADC and NetScaler Gateway version 12.1 is now End Of Life and is vulnerable.

Impact

The impacts of exploitation of these vulnerabilities are as follows:

- CVE-2023-3519: Could allow an unauthenticated remote attacker to execute remote code on the appliance.
- CVE-2023-3466: Could allow an attacker to perform reflected XSS attacks in order to reflect a malicious script off of a web application to the victim's browser.
- CVE-2023-3467: Could provide an attacker with privilege escalation to root administrator.

Recommendations

The NCSC strongly advises affected organisations to identify any vulnerable appliances and upgrade to one of the supported versions provided by Citrix that will address these vulnerabilities.

Further information and some steps that organisations can take can be found here:
https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467

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