National Cyber Security Centre

0811221956-NCSC

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

NCSC Alert

Critical Vulnerabilities in Citrix Gateway and Citrix ADC (CVE-2022-27510, CVE-2022-27513 and CVE-2022-27516)

Tuesday 8th November, 2022

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

Vulnerabilities have been discovered in Citrix Gateway and Citrix ADC, listed below. Note that only appliances that are operating as a Gateway (appliances using the SSL VPN functionality or deployed as an ICA proxy with authentication enabled) are affected by the first issue, which is rated as a Critical severity vulnerability.

CVE-ID	CWE	Affected Products	Pre-conditions
CVE-2022-27510	CWE-288: Authentication Bypass Using an Alternate Path or Channel	Citrix Gateway, Citrix ADC	Appliance must be configured as a VPN Gateway
CVE-2022-27513	CWE-345: Insufficient Verification of Data Authenticity	Citrix Gateway, Citrix ADC	Appliance must be configured as a VPN Gateway & the RDP proxy functionality must be configured
CVE-2022-27516	CWE-693: Protection Mechanism Failure	Citrix Gateway, Citrix ADC	Appliance must be configured as a VPN Gateway OR a AAA virtual server, and the user lockout functionality “Max Login Attempts” must be configured

You can view the Citrix advisory here: https://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve202227510-cve202227513-and-cve202227516.

Products Affected

- Citrix ADC and Citrix Gateway 13.1 before 13.1-33.47
- Citrix ADC and Citrix Gateway 13.0 before 13.0-88.12
- Citrix ADC and Citrix Gateway 12.1 before 12.1.65.21
- Citrix ADC 12.1-FIPS before 12.1-55.289
- Citrix ADC 12.1-NDcPP before 12.1-55.289

This bulletin only applies to customer-managed Citrix ADC and Citrix Gateway appliances. Citrix customers using Citrix-managed cloud services do not need to take any action.

Impact

- CVE-2022-27510: Unauthorized access to Gateway user capabilities
- CVE-2022-27513: Remote desktop takeover via phishing
- CVE-2022-27516: User login brute force protection functionality bypass

Recommendations

The NCSC strongly advises affected customers of Citrix ADC and Citrix Gateway to iinstall the relevant updated versions of Citrix ADC or Citrix Gateway as soon as possible:

- Citrix ADC and Citrix Gateway 13.1-33.47 and later releases
- Citrix ADC and Citrix Gateway 13.0-88.12 and later releases of 13.0
- Citrix ADC and Citrix Gateway 12.1-65.21 and later releases of 12.1
- Citrix ADC 12.1-FIPS 12.1-55.289 and later releases of 12.1-FIPS
- Citrix ADC 12.1-NDcPP 12.1-55.289 and later releases of 12.1-NDcP

Please note that Citrix ADC and Citrix Gateway versions prior to 12.1 are EOL and customers on those versions are recommended to upgrade to one of the supported versions.

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