NCSC

National Cyber Security Centre

2212131247-NCSC

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

NCSC Alert

Critical Vulnerabilities in Citrix Gateway and Citrix ADC (CVE-2022-27518)

Tuesday 13th December, 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

A critical vulnerability has been discovered in Citrix Gateway and Citrix ADC appliances, that, if exploited, could allow an unauthenticated remote attacker to perform arbitrary code execution on the appliance. Exploitation of CVE-2022-27518 on unmitigated appliances in the wild have been reported.

You can view the Citrix advisory here: https://support.citrix.com/article/CTX474995/citrix-adc-and-citrix-gateway-security-bulletin-for-cve202227518. In order for the vulnerability to be successfully exploited, the following pre-condition must be met: The Citrix ADC or Citrix Gateway must be configured as a SAML SP or a SAML IdP.

Products Affected

The following versions of Citrix ADC and Citrix Gateway are affected by this vulnerability if the pre-condition is met:

- Citrix ADC and Citrix Gateway 13.0 before 13.0-58.32
- Citrix ADC and Citrix Gateway 12.1 before 12.1-65.25
- Citrix ADC 12.1-FIPS before 12.1-55.291
- Citrix ADC 12.1-NDcPP before 12.1-55.291

Citrix ADC and Citrix Gateway version 13.1 are unaffected by this vulnerability.

Citrix customers can determine if their Citrix ADC or Citrix Gateway is configured as a SAML SP or a SAML IdP by inspecting the ns.conf file for the following commands:

```
add authentication samlAction
```

- The appliance is configured as a SAML SP

OR

```
add authentication samlIdPProfile
```

- The appliance is configured as a SAML IdP

If either of the commands are present in the ns.conf file and if the version is an affected version, then the appliance should be updated as soon as practicable. Citrix customers using Citrix-managed cloud services do not need to take any action.

Impact

Exploitation of CVE-2022-27518 could allow an attacker to remotely execute code and carry out data theft, operational disruption, ransomware and denial of service.

Recommendations

Citrix has strongly urged affected customers of Citrix ADC and Citrix Gateway to install the relevant updated versions of Citrix ADC or Citrix Gateway as soon as possible:

- Citrix ADC and Citrix Gateway 13.0-58.32 and later releases
- Citrix ADC and Citrix Gateway 12.1-65.25 and later releases of 12.1
- Citrix ADC 12.1-FIPS 12.1-55.291 and later releases of 12.1-FIPS
- Citrix ADC 12.1-NDcPP 12.1-55.291 and later releases of 12.1-NDcPP

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.

For additional information, including IOCs and mitigation steps, please also refer to the threat hunting guidance document for Citrix ADC published by the US NSA:
https://media.defense.gov/2022/Dec/13/2003131586/-1/-1/0/CSA-APT5-CITRIXADC-V1.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