National Cyber Security Centre

201912311241-NCSC

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

NCSC Advisory

Citrix NetScaler (ADC) Vulnerability CVE-2019-19781
2019-12-31

Status: TLP-WHITE

NCSC

Traffic Light Protocol

This document is classified using Traffic Light Protocol. Recipients may share TLP: WHITE information freely, 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.

Technical Detail

1. Overview

Threat Type	A serious vulnerability has been found in Citrix Application Delivery Controller (formerly known as NetScaler) and Citrix Gateway. This vulnerability, if exploited, could allow unauthenticated attackers to perform arbitrary code execution.
Systems Affected	The vulnerability affects all supported product versions and all supported platforms: - Citrix ADC and Citrix Gateway version 13.0 all supported builds - Citrix ADC and NetScaler Gateway version 12.1 all supported builds - Citrix ADC and NetScaler Gateway version 12.0 all supported builds - Citrix ADC and NetScaler Gateway version 11.1 all supported builds - Citrix NetScaler ADC and NetScaler Gateway version 10.5 all supported builds
Impact	Arbitrary Code Execution
Recommendations	Citrix has provided mitigation steps that affected customers can apply immediately, details can be found at the following URL: https://support.citrix.com/article/CTX267679/. They also advise that customers then upgrade all of their vulnerable appliances to a fixed version of the appliance firmware when released.

2. Description

On 17th December 2019 Citrix released a critical security bulletin (CTX267027) advising users of a vulnerability that exists on their Citrix Application Delivery Controller (formerly known as NetScaler) and Citrix Gateway. The impact of the vulnerability has become more apparent since then.
These devices are used in many organisations as load balancers, to control access to APIs and to terminate SSL VPNs for remote access etc. It is believed that circa 80,000 organisations are affected worldwide by the vulnerability.

The vulnerability appears to take advantage of a flaw that allows attackers to traverse directories, potentially allowing them to access files and directories that are stored outside the web root folder.

CSIRT-IE advises constituents to follow the advice given by Citrix and apply the mitigation steps as detailed in the URL provided in the section below (Mitigation). Also, as this vulnerability appears to have been present for some time, constituents should attempt to detect past exploitation of the flaw.

3. Mitigation

Citrix has advised users to apply configuration changes to serve as a mitigation as outlined in the URL below:
`https://support.citrix.com/article/CTX267679`

A number of Proof of Concept (POC) exploits have now been publicly released and reports indicate a marked increase in scanning activity associated with the vulnerability.

Citrix has announced that they are working on permanent fixes for this vulnerability and will make them available for supported versions as follows:

Version 13: 27-Jan-2020
Version 12.1: 27-Jan-2020
Version 12: 20-Jan-2020
Version 11.1: 20-Jan-2020
Version 10.5: 31-Jan-2020

CSIRT-IE strongly advises owners of these devices to apply the mitigation outlined by Citrix as a matter of urgency and when available, apply the permanent firmware upgrades.

Feedback and Reporting

NCSC-IE wishes to offer whatever assistance it can in relation to this incident and is willing to work with the relevant parties to further understand the current threat. NCSC-IE would also request any feedback in relation to this incident as regards the relevance and accuracy of the information provided.