FOX IT
part of nccgroup

CLASSIFICATION
PUBLIC

InTELL Threat Advisory

Advisory on Citrix vulnerability CVE-2019-19781

FOR A
MORE
SECURE
SOCIETY

Overview of possible Citrix mitigation steps

Fox-IT noticed a lot of companies and organizations struggling to decide what steps need to be taken to mitigate risks regarding Citrix [1], following the latest updates from Citrix [2][3] as well as NCSC NL [5]. Their main question is: “Do we need to take down all devices?” The mitigation steps to reduce risks as much as possible depends (among others) on the version of Citrix used by your organization or company. This article provides an overview of the scenarios' and mitigations steps currently published by Citrix, some guidance for further impact assessment and investigation, as well as the latest update from NCSC-NL.

Citrix published [2] one set with mitigation measure for vulnerability CVE-2019-19781 [1] which should be sufficient for all affected Citrix versions and builds as indicated on their website. However, it is important to note that there is an exception for Citrix ADC Release 12.1 builds before 51.16/51.19 and 50.31. Citrix indicates the following about this specific version and builds:

> '***In Citrix ADC Release 12.1 builds before 51.16/51.19 and 50.31, a bug exists that affects responder and rewrite policies bound to VPN virtual servers causing them not to process the packets that matched policy rules. Citrix recommends customers update to an unaffected build for the mitigation steps to apply properly.***'

This means that there are 2 generic scenarios to implement the mitigation measures, which are further outlined in the table below.

	Mitigation scenario 1	Mitigation scenario 2

Version of Citrix	• Citrix ADC and Citrix Gateway version 13.0 all supported builds
	• Citrix ADC and NetScaler Gateway version 12.1 all supported builds (for build before 50.31, 51.16/51.19, see **scenario 2**)
	• 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
	• Citrix SD-WAN WANOP software and appliance models
		• Citrix ADC release 12.1 with builds before:
		  ○ Build 50.31
		  ○ Build 51.16/51.19

	Mitigation scenario 1	Mitigation scenario 2
	4000, 4100, 5000, and 5100 all supported builds	
Mitigation steps	1. Check if your Citrix version matches with the Citrix version for this scenario 2. Apply mitigation steps according to the mitigation advice of Citrix [2] 3. Verify whether the performed mitigation steps were successful [3]	1. Check if your Citrix version matches with the Citrix version for this scenario 2. Upgrade your Citrix to a version/ build to (see Citrix versions mentioned under scenario 1) make sure that the mitigation steps will be effective. If it is not possible for a variety of reasons to perform the upgrade, see also the below 'Risk assessment' section. 3. Apply mitigation steps according to the mitigation advice of Citrix [2] 4. Verify whether the performed mitigation steps were successful [3]

Impact assessment/ alternative (partial) detection/ mitigation steps

Citrix ADC release 12.1 with builds before build 50.31, or build 51.16/51.19 (scenario 2) need an upgrade to successfully implement the suggested mitigation steps, according to Citrix. If this is not possible for a variety of reasons, those who are impacted by this, need to assess what the impact and risk might be of an alternative /detection mitigation scenario for themselves, due to the fact that this is a business decision.

- Whitelisting IP's: in case the Citrix device can't be upgraded a strict whitelist of IP's can be maintained to fence of the Citrix for the greater public. However, please keep in mind that the device remains vulnerable and a residual risk still exists. Organizations themselves should perform a risk assessment to determine their risk appetite and whether this is a realistic scenario for them.
- Extensive monitoring: additionally to whitelisting incoming IP's, monitoring the device extensively for traces of a compromise would be a recommended step. Do note that just network based monitoring is not sufficient and continuously monitoring of (among others) the log files is required.
- Turning off the device: turning off the device will mitigate the risk of being compromised and the vulnerability being exploited. However, whether this is an option for an organization is depending on the situation and again a risk assessment is required to determine whether this is realistic scenario, taking into account the risk appetite, economic damage etc.

Check for traces of a compromise

It hasn't been clear for every organization with a Citrix ADC release 12.1 with builds before 51.16/51.19 or 50.31, that an upgrade was required to make the mitigation steps effective. Meaning that although they might have followed the mitigation steps in an earlier stage, they were still vulnerable for this CVE. Therefore, it is always recommended to check for traces of a compromise on your Citrix device. This

does not only apply for the earlier mentioned organizations, but for those organization who waited too long with following the mitigation steps after the release of the public exploit code on the 10th of January, 2020 as well. Another security company published [4] a blogpost to check for forensics artifacts to find indicators that the vulnerability might have been successfully exploited.

NCSC NL advisory

The Dutch National Cyber Security Center (NCSC), published [5] an updated advisory on the 16th of January, 2020, indicating that the mitigation measures as proposed by Citrix might not always be effective and that there is uncertainty about the effectiveness of the mitigation measures. This is only being confirmed by Citrix for specific versions of Citrix ADC release 12.1 with builds before build 50.31, or build 51.16/51.19 [2]. Although Citrix states that for the corresponding earlier mentioned builds an upgrade is required which should make the mitigation steps effective again, NCSC indicates that the upgrade is not a guarantee that the proposed mitigation steps are an adequate solution without providing further details at the moment.

It's unclear to Fox-IT, based on the article of NCSC NL, whether the mitigation steps aren't an adequate solution for all vulnerable Citrix devices that are vulnerable for CVE-2019-19781. Fox-IT hasn't observed any detailed proof from NCSC that confirms/rejects the statement of NCSC NL in general. In one of our investigations we have seen that implementing the supplied technical measurements by Citrix, resulted in a specific Citrix ADC product being no longer vulnerable to the currently public available exploit. Therefore it remains difficult for Fox-IT to validate the accuracy with the lack of technical details of this statement in general and we are recommending the earlier mentioned mitigation scenarios provided by Citrix nonetheless. The official statement of Citrix (based on an interview of ZDnet [6] with the Citrix CISO) of the 16th of January, 2020 remains the same:

"The mitigations we published cover all supported versions of our software and contain detailed steps designed to stop a potential attack across all known scenarios. But all steps must be followed," and "We continue to recommend that our customers apply the mitigation immediately - and the permanent fixes when they become available."

Fox-IT will continue to monitor for updates about the provided effectiveness/ adequacy of the Citrix mitigation steps. Significant updates on this article will be pushed to Fox-IT MDR customers via our portal. Other interested parties are advised to check our website on updates regularly. More important news on this matter could be expected and therefore Fox-IT advises to monitor the website of NCSC NL for more updates in parallel.

[1] https://support.citrix.com/article/CTX267027
[2] https://support.citrix.com/article/CTX267679
[3] https://support.citrix.com/article/CTX269180
[4] https://www.trustedsec.com/blog/netscaler-remote-code-execution-forensics
[5] https://www.ncsc.nl/actueel/nieuws/2020/januari/16/door-citrix-geadviseerde-mitigerende-maatregelen-niet-altijd-effectief
[6] https://www.zdnet.com/google-amp/article/a-hacker-is-patching-citrix-servers-to-maintain-exclusive-access/

Terms of Use

InTELL tracks global cybercrime activity. We base our intelligence on tracking threat actors, darkweb research, forensic investigations, internationally deployed sensors and fraud monitoring services. Going beyond botnet & malware information, we provide a global picture of trends, geographical activity, actors, their motivations and their evolving business models. We provide links to campaigns, tactics, procedures and individual IoCs to feed network security components. Customers become part of a global community, with live threat tracking, collaboration, and the largest criminal threat database, with over a decade of experience.

The data and charts contained within this report represents Fox-IT's own dataset collected within its malware lab. The data from this lab should be considered a sample including factors potentially skewing the analysis: our lab does not analyze every malware sample in the threat landscape, merely those assessed to represent a crosssection from a variety of sources. Our sources may be skewed towards certain types, families or regions which can introduce further bias. The report documents the dataset over a fixed period of time allowing for comparative analysis, whereas when referring to previous datasets a discrepancy with previous reports may seemingly occur due to inclusion of the updated dataset that may contain recent data impacting the statistical outcome.

Furthermore, the lists of data we use to identify targets for attacks can also be biased because they will naturally contain more data pertaining to Fox-IT customers than organizations not part of the InTELL community. Although we augment customer supplied data (such as URLs for online banking and BINs) with autonomously collected data, the customer supplied data will always be more detailed and extensive. In short, these charts provide indications, and should be incorporated by interested parties as such. Customers are advised to incorporate and correlate multiple feeds with internal network telemetry.

Fox-IT

Fox-IT prevents, solves and mitigates the most serious threats caused by cyber attacks, data leaks, or fraud with innovative solutions for governments, defense agencies, law enforcement, critical infrastructure and banking and commercial enterprise clients worldwide. Fox-IT combines smart ideas with advanced technology to create solutions that contribute to a more secure society.
We develop products and custom solutions for our clients to guarantee the safety of sensitive and critical government systems, to protect industrial networks, to defend online banking systems, and to secure confidential data.

For more detailed information about Fox-IT, including partner details, please go to www.fox-it.com

CLASSIFICATION
PUBLIC

FOX IT
part of nccgroup

fox-it.com

Fox-IT
Olof Palmestraat 6, Delft
P.O. Box 638, 2600 AP Delft
The Netherlands

Fox-it is part of ncc-group.

T +31 (0)15 284 7999
F +31 (0)15 284 7990
intell@fox-it.com
cybercrime-portal.fox-it.com
fox@fox-it.com