



| Flash |

Citrix Vulnerabilities Continue to Be Exploited

F-2024-01-17c

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Vulnerability Exploitation, Zero-day

January 17, 2024

Scope Note: ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 12:00 PM (EST) on January 17, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Citrix Vulnerabilities Continue to Be Exploited

› Key Findings

- Threat actors continue to exploit three separate Citrix vulnerabilities relating to Netscaler Application Delivery Controller (ADC) and Gateway appliances, which is likely indicative of a significant number of networks comprising this equipment remaining unpatched.
- On January 16, 2024, Citrix urged consumers to update software relating to actively-exploited zero-day vulnerabilities CVE-2023-6548 and CVE-2023-6549.¹
- An article published on January 14, 2024, in dark web forum xss. provides instructions on how CVE-2023-4966 can be exploited, with its reception being indicative of a continued interest amongst threat actors.

| Details

On January 16, 2024, Citrix released a security bulletin urging consumers to update Netscaler ADC and Gateway appliances to mitigate against actively-exploited zero-day vulnerabilities CVE-2023-6548 and CVE-2023-6549, which impact the Netscaler management interface.

¹

[hXXps://support.citrix\[.\]com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549](https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549)

- If unpatched, the former enables an attacker to conduct remote code execution, and the latter can be leveraged in denial-of-service (DoS) attacks.

According to Citrix, the following versions of Netscaler ADC (formerly Citrix ADC) and Netscaler Gateway (formerly Citrix Gateway) are affected by the vulnerabilities:

- Netscaler ADC and Netscaler Gateway 14.1 before 14.1-12.35
- Netscaler ADC and Netscaler Gateway 13.1 before 13.1-51.15
- Netscaler ADC and Netscaler Gateway 13.0 before 13.0-92.21
- Netscaler ADC 13.1-FIPS before 13.1-37.176
- Netscaler ADC 12.1-FIPS before 12.1-55.302
- Netscaler ADC 12.1-NDcPP before 12.1-55.302

CVE-2023-4966, also known as “Citrix Bleed,” is also very likely still being targeted by threat actors. An article published as early as January 14, 2024, in dark web forum xss. is very likely indicative of a significant number of networks comprising Citrix Netscaler and Gateway appliances remaining unpatched and vulnerable to the critical vulnerability.

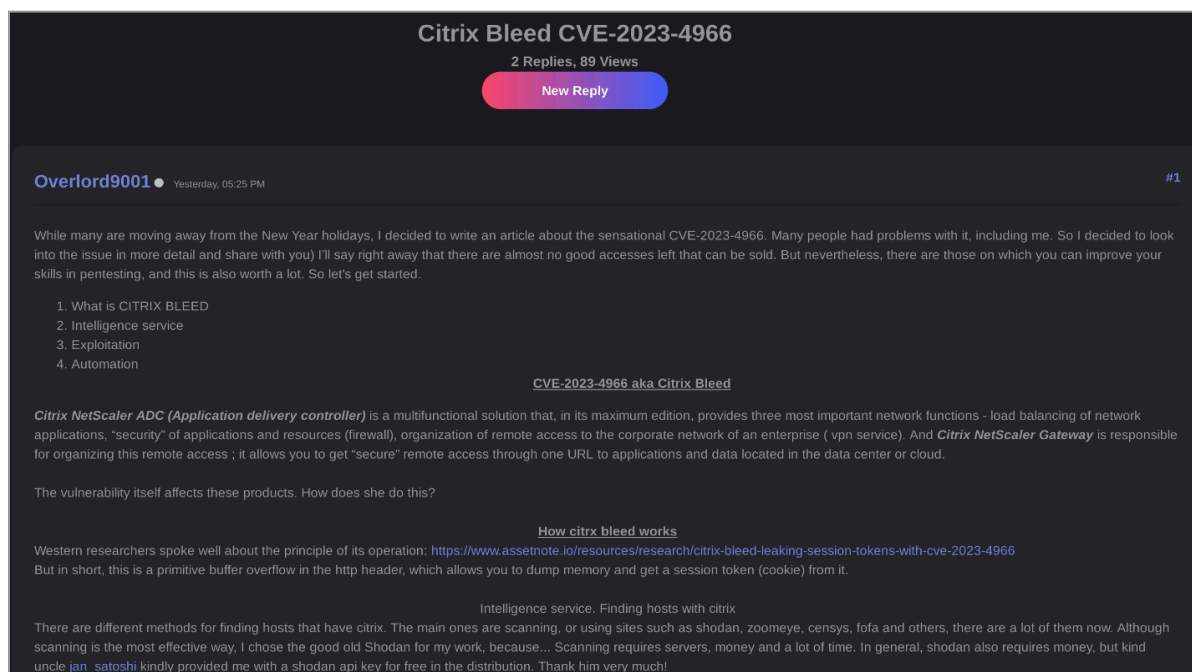
The article is translated from an existing Russian publication and advises readers on:

- Finding and studying potential targets via open source search engine Shodan;
- Subsequently exploiting them via the use of “Choccapikk”—a tool readily available on developer platform GitHub; and
- Automating and replicating the attack process in order to exploit as many targets as possible.

The article was posted by a well-regarded threat actor in xss. known as “Overlord9001” and received significant acclaim from both English and Russian-speaking actors.

- The notably positive reception of this article very likely indicates that threat actors still seek to exploit CVE-2023-4966.
- Despite its prominent reputation within deep and dark web (DDW) forums, many threat actors likely experience difficulties in leveraging the vulnerability to conduct

subsequent attacks, such as gaining access to data centers associated with Citrix Netscaler appliances.



Screenshot of the article's introductory paragraphs

Source: ZeroFox Intelligence

CVE-2023-4966 is a critical-severity, remotely-exploitable security flaw that enables attackers to retrieve authentication session cookies from vulnerable Citrix Netscaler ADC and Gateway appliances. This can lead to the bypass of multi-factor authentication protocols and session hijacking, allowing subsequent network attacks to take place.

It was discovered and patched by Citrix on October 10, 2023, though significant exploitation took place both before its discovery and in the months following the patch's release. The vulnerability almost certainly continues to appeal to a variety of threat actors, including:

- Initial access brokers (IABs);
- Advanced Persistent Threat (APT) groups, such as FIN8; and
- Financially-motivated ransomware collectives, such as LockBit, MedusaLocker, and ALPHV—all of which have almost certainly exploited CVE-2023-4966 to conduct digital extortion campaigns.

We automate the process

It turns out that driving in cookies is a very exhausting task. Yes, it's interesting, but switching all these tabs and copying back and forth... And when there's nothing on the target yet... Monkey's work in general.

But that's why we're hackers, to automate the routine, and then get access and get high null

Therefore, for these purposes, let's add an exploit from Chocapikk to additionally perform the following actions:

1. When a target with valid cookies is found, a browser window will open, in which a citrix session with our cookies will open. We will do this through the selenium library. Also, using the threading library, we will create a semaphore to synchronize our sessions. So that our virtual machine or vps does not fall short of the number of accesses)
2. All IP users that are vulnerable to citrix bleed will be recorded in the new txt. Regardless of whether the cookies are valid or not. This is necessary in order to re-use citrix bleed on these targets in the future, because our access depends on whether the corporate employee is working.

Here's the code:

```
# https://github.com/Chocapikk/CVE-2023-4966

import re
import sys
import hexdump
import argparse
import requests

from rich.console import Console
from urllib.parse import urlparse
from alive_progress import alive_bar
from typing import List, Tuple, Optional, TextIO
from concurrent.futures import ThreadPoolExecutor, as_completed

warnings = requests.packages.urllib3
warnings.disable_warnings(warnings.exceptions.InsecureRequestWarning)

class CitrixMemoryDumper:
```

Guidance on process automation

Source: ZeroFox Intelligence

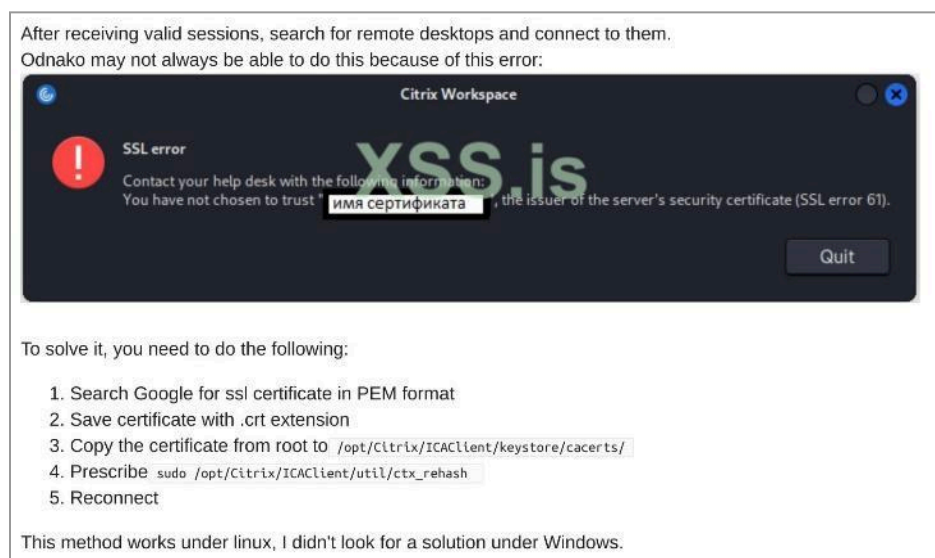
The article contains information that is likely intended to appeal particularly to ransomware collectives, due to the detail provided on delivering malicious payloads after gaining initial network access.

- This likely highlights continued interest in the Citrix Bleed vulnerability from ransomware and digital extortion (R&DE) collectives.
- There is a roughly even chance that newer, highly-active R&DE collectives observed during 2023, which are likely comprised of some less experienced operatives of a lower technical sophistication, will benefit the most from guides such as these.

One aspect of the original article is not included in this translation. The missing section advises potential attackers on how to deal with an SSL error returned by Citrix Workspace upon attempting to connect to a remote desktop, which is noted as an effect of the

successful implementation of the guide. The actor claims that, if the attack is conducted on operating system Linux, the process to circumvent this error is as follows:

- Obtain an SSL certificate in PEM format, via an open source search engine;
- Change its extension to [.]crt;
- Copy it into a recognized/opt subfolder (i.e., the directory that contains non-default software packages); and
- Update the certificate store used by the Citrix client—a readily available and effective solution that could enable further attacks via Citrix Bleed.



Guidance upon encountering SSL error

Source: ZeroFox Intelligence

The recent security bulletin from Citrix is very likely indicative of the continued targeting of Citrix Netscaler ADC and Netscaler Gateway appliances via the exploitation of CVE-2023-6548 and CVE-2023-6549. The publication is likely to prompt some consumers to install the latest security patches, but it is likely that additional attacks will continue.

Should the article guiding the exploitation of CVE-2023-4966 prove intuitive and effective, it is likely that associated attacks will continue during the short term. Citrix Bleed is very likely to appeal to newer, financially-motivated R&DE collectives that previously lacked the technical expertise to exploit this vulnerability, as well as larger

groups seeking to capitalize upon the likely sizable number of networks that have not been patched with the latest software.

| Recommendations

- Ensure networks featuring Citrix Netscaler and Gateway appliances are patched with the latest Citrix patches and adhere to the relevant recommendations.
 - [hXXps://www.netscaler\[.\]com/blog/news/netscaler-investigation-recommendations-for-cve-2023-4966/](https://www.netscaler.com/blog/news/netscaler-investigation-recommendations-for-cve-2023-4966/)
 - [hXXps://docs.netscaler\[.\]com/en-us/netscaler-adc-secure-deployment.html](https://docs.netscaler.com/en-us/netscaler-adc-secure-deployment.html)
 - [hXXps://www.citrix\[.\]com/downloads/](https://www.citrix.com/downloads/)
- Ensure a thorough understanding of organizational technology stacks, including those of operating partners.
- Consistently monitor for security patch releases impacting these products, and deploy a holistic patch management system to ensure all business IT assets are updated with the latest software as quickly as possible.
- Conduct a thorough assessment of servers and review any relevant activity logs for suspicious behavior.
- Leverage CISA's KEV catalog to prioritize out-of-cycle vulnerability patching.
- Protect endpoint devices with phishing-resistant MFA protocols compliant with FIDO2 or PKI standards.
- Ensure critical data is backed up to secure off-site or cloud servers. Sensitive or proprietary data should be properly compartmentalized, avoiding aggregation or unnecessary accumulation.
- Use the ZeroFox Platform's Intelligence Search capability to investigate vulnerabilities and associated exploits.
- Maintain a clear and comprehensive incident response strategy consisting of business resilience and continuity plans, incident reporting procedures and key authorities.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%