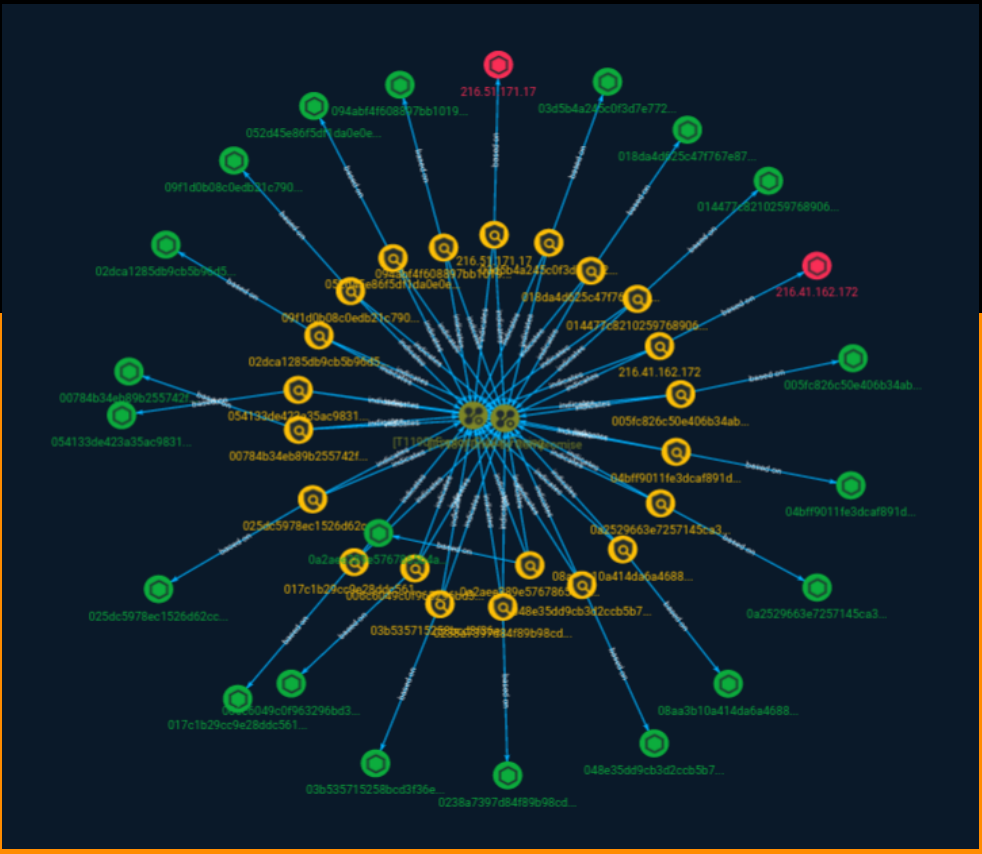
Jul 20 2023

NETMANAGEIT

# Intelligence Report

# Critical and High Vulnerabilities in Citrix ADC and Citrix Gateway (CVE-2023-3519, CVE-2023-3466, CVE-2023-3467)



# Table of contents

## Overview

## Entities

## Observables

## External References

# Overview

## Description

Citrix ADC and Citrix Gateway, widely used for secure application delivery and remote access solutions, are found to have critical vulnerabilities. These vulnerabilities pose significant risks, including privilege escalation and remote code execution. Exploits of the unauthenticated remote code execution vulnerability have already been observed.

## Confidence

*This value represents the confidence in the correctness of the data contained within this report.*

15 / 100

# Indicator

**Name**

094abf4f608897bb1019e0f400669af6573c298ce0a9fc9ee3fd3490a12a31ab

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' =
'094abf4f608897bb1019e0f400669af6573c298ce0a9fc9ee3fd3490a12a31ab']

**Name**

03b535715258bcd3f36e78df21d624109b4d3b06a24317f457237eb58f41af53

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' =
'03b535715258bcd3f36e78df21d624109b4d3b06a24317f457237eb58f41af53']

**Name**

04bff9011fe3dcaf891dd712b74dab4e0405bbcafb2122c8a130395145f562fa

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '04bff9011fe3dcaf891dd712b74dab4e0405bbcafb2122c8a130395145f562fa']

**Name**

017c1b29cc9e28ddc5615617d9b08bba0c142a2382533bf8e19f6e038483d209

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '017c1b29cc9e28ddc5615617d9b08bba0c142a2382533bf8e19f6e038483d209']

**Name**

09f1d0b08c0edb21c790ad4600dc6ddb675cb117a8f8ca3d4d34e98987235189

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' =
'09f1d0b08c0edb21c790ad4600dc6ddb675cb117a8f8ca3d4d34e98987235189']

**Name**

005fc826c50e406b34abf5c86a8b9f3dee2791ec0783d50415015188f4f566f6

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' =
'005fc826c50e406b34abf5c86a8b9f3dee2791ec0783d50415015188f4f566f6']

**Name**

025dc5978ec1526d62cc44c58600435ead5aa5d11a65abd6d4164a6bce93f422

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' =
'025dc5978ec1526d62cc44c58600435ead5aa5d11a65abd6d4164a6bce93f422']

**Name**

02dca1285db9cb5b96d51fd8ff64f25d023802fb18118888a67793a3b6351cda

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '02dca1285db9cb5b96d51fd8ff64f25d023802fb18118888a67793a3b6351cda']

**Name**

08aa3b10a414da6a4688a6217e318a7fa424ffc28a687f269bbc38a4beedc367

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '08aa3b10a414da6a4688a6217e318a7fa424ffc28a687f269bbc38a4beedc367']

**Name**

006c6049c0f963296bd33e292624dbb26c0e8e843336bbc367adedd30cfce5e3

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '006c6049c0f963296bd33e292624dbb26c0e8e843336bbc367adedd30cfce5e3']

**Name**

216.41.162.172

**Description**

CC=US ASN=AS53435 JACKSONENERGY-EPL

**Pattern Type**

stix

**Pattern**

[ipv4-addr:value = '216.41.162.172']

**Name**

0a2529663e7257145ca303183937b0f6b4cee4c9cbdab665ad87fe4171f77551

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '0a2529663e7257145ca303183937b0f6b4cee4c9cbdab665ad87fe4171f77551']

**Name**

00784b34eb89b255742ff13ea41eb2e5cdd444a7d0053eabb247925b2c551252

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '00784b34eb89b255742ff13ea41eb2e5cdd444a7d0053eabb247925b2c551252']

**Name**

03d5b4a245c0f3d7e772a8ef61d199ebc669d5579efb18e6ef494830f3acae0e

**Description**

Backdoor:Win32/Tofsee.T

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '03d5b4a245c0f3d7e772a8ef61d199ebc669d5579efb18e6ef494830f3acae0e']

**Name**

0238a7397d84f89b98cd66db267d8af52ff134ac79bfe4196d32b0aaf6534449

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '0238a7397d84f89b98cd66db267d8af52ff134ac79bfe4196d32b0aaf6534449']

### Name

216.51.171.17

### Description

**ISP:** Aureon Network Services **OS:** None ------------------------- Hostnames: - blfd-11-static-216-51-171-17.dsl.netins.net ------------------------- Domains: - netins.net ------------------------- Services: **5150:** ``` NUSP/1.0 500 CSeq: 0 ``` ------------------ **8444:** ``` HTTP/1.1 200 OK X-Powered-By: PHP/5.6.32 Set-Cookie: PHPSESSID=c4ab5695eca111d5f85f9cd91d87c78b; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Content-type: text/html; charset=UTF-8 Content-Length: 11871 Date: Sat, 08 Jul 2023 22:34:16 GMT Server: lighttpd/1.4.48 ``` ------------------

### Pattern Type

stix

### Pattern

[ipv4-addr:value = '216.51.171.17']

### Name

0a2aee389e5767865b4a3f83e267282d92316b37c5288ae3786e2826d576debd

### Pattern Type

stix

### Pattern

[file:hashes.'SHA-256' = '0a2aee389e5767865b4a3f83e267282d92316b37c5288ae3786e2826d576debd']

| |
|---|
| **Name** |
| 018da4d625c47f767e8765c59626b522e7a2eec3788062651070b83e49c0a514 |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.'SHA-256' = '018da4d625c47f767e8765c59626b522e7a2eec3788062651070b83e49c0a514'] |
| **Name** |
| 052d45e86f5df1da0e0ebeaf166cb2f69b7e710dfd0ffd3fb9507085cd554183 |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.'SHA-256' = '052d45e86f5df1da0e0ebeaf166cb2f69b7e710dfd0ffd3fb9507085cd554183'] |
| **Name** |
| 048e35dd9cb3d2ccb5b75e2f56e0558cf8343d8a0409127fc89611d75acceb08 |
| **Pattern Type** |
| stix |
| **Pattern** |

[file:hashes.'SHA-256' =
'048e35dd9cb3d2ccb5b75e2f56e0558cf8343d8a0409127fc89611d75acceb08']

**Name**

054133de423a35ac98311cb0fb6b39ea1bc912be6a89b9a865ce1a0c68c82527

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' =
'054133de423a35ac98311cb0fb6b39ea1bc912be6a89b9a865ce1a0c68c82527']

**Name**

014477c82102597689066df18380f2ac84998ccdacf3833add2bb223dfd512d0

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' =
'014477c82102597689066df18380f2ac84998ccdacf3833add2bb223dfd512d0']

# Attack-Pattern

**Name**

Drive-by Compromise

**ID**

T1189

**Description**

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring [Application Access Token](https://attack.mitre.org/techniques/T1550/001). Multiple ways of delivering exploit code to a browser exist (i.e., [Drive-by Target](https://attack.mitre.org/techniques/T1608/004)), including: * A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting * Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary * Malicious ads are paid for and served through legitimate ad providers (i.e., [Malvertising](https://attack.mitre.org/techniques/T1583/008)) * Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content). Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.(Citation: Shadowserver Strategic Web Compromise) Typical drive-by compromise process: 1. A user visits a website that is used to host the adversary controlled content. 2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version. * The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes. 3. Upon finding a vulnerable version, exploit code is delivered to the browser. 4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place. * In some cases a second visit to the website after the initial scan is required before exploit code is delivered. Unlike [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ. Adversaries may also use compromised websites to deliver a user to a malicious application designed to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s, like OAuth tokens, to gain access to protected applications and information. These malicious applications have been delivered through popups on legitimate websites.(Citation: Volexity OceanLotus Nov 2017)

**Name**

Exploit Public-Facing Application

**ID**

T1190

**Description**

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation:

Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities. (Citation: OWASP Top 10)(Citation: CWE top 25)

# StixFile

| Value |
|---|
| 02dca1285db9cb5b96d51fd8ff64f25d023802fb18118888a67793a3b6351cda |
| 09f1d0b08c0edb21c790ad4600dc6ddb675cb117a8f8ca3d4d34e98987235189 |
| 08aa3b10a414da6a4688a6217e318a7fa424ffc28a687f269bbc38a4beedc367 |
| 017c1b29cc9e28ddc5615617d9b08bba0c142a2382533bf8e19f6e038483d209 |
| 018da4d625c47f767e8765c59626b522e7a2eec3788062651070b83e49c0a514 |
| 00784b34eb89b255742ff13ea41eb2e5cdd444a7d0053eabb247925b2c551252 |
| 0a2aee389e5767865b4a3f83e267282d92316b37c5288ae3786e2826d576debd |
| 048e35dd9cb3d2ccb5b75e2f56e0558cf8343d8a0409127fc89611d75acceb08 |
| 052d45e86f5df1da0e0ebeaf166cb2f69b7e710dfd0ffd3fb9507085cd554183 |
| 03d5b4a245c0f3d7e772a8ef61d199ebc669d5579efb18e6ef494830f3acae0e |
| 0238a7397d84f89b98cd66db267d8af52ff134ac79bfe4196d32b0aaf6534449 |
| 025dc5978ec1526d62cc44c58600435ead5aa5d11a65abd6d4164a6bce93f422 |
| 005fc826c50e406b34abf5c86a8b9f3dee2791ec0783d50415015188f4f566f6 |

03b535715258bcd3f36e78df21d624109b4d3b06a24317f457237eb58f41af53

014477c82102597689066df18380f2ac84998ccdacf3833add2bb223dfd512d0

04bff9011fe3dcaf891dd712b74dab4e0405bbcafb2122c8a130395145f562fa

006c6049c0f963296bd33e292624dbb26c0e8e843336bbc367adedd30cfce5e3

0a2529663e7257145ca303183937b0f6b4cee4c9cbdab665ad87fe4171f77551

054133de423a35ac98311cb0fb6b39ea1bc912be6a89b9a865ce1a0c68c82527

094abf4f608897bb1019e0f400669af6573c298ce0a9fc9ee3fd3490a12a31ab

# IPv4-Addr

| Value |
|---|
| 216.51.171.17 |
| 216.41.162.172 |

# External References

- https://otx.alienvault.com/pulse/64b9335ce8519e9f539f2e27
- https://socradar.io/critical-and-high-vulnerabilities-in-citrix-adc-and-citrix-gateway-cve-2023-3519-cve-2023-3466-cve-2023-3467/