Oct 15 2023

NETMANAGEIT

Intelligence Report

Nation-state Hackers Exploiting Confluence Zero-day Vulnerability

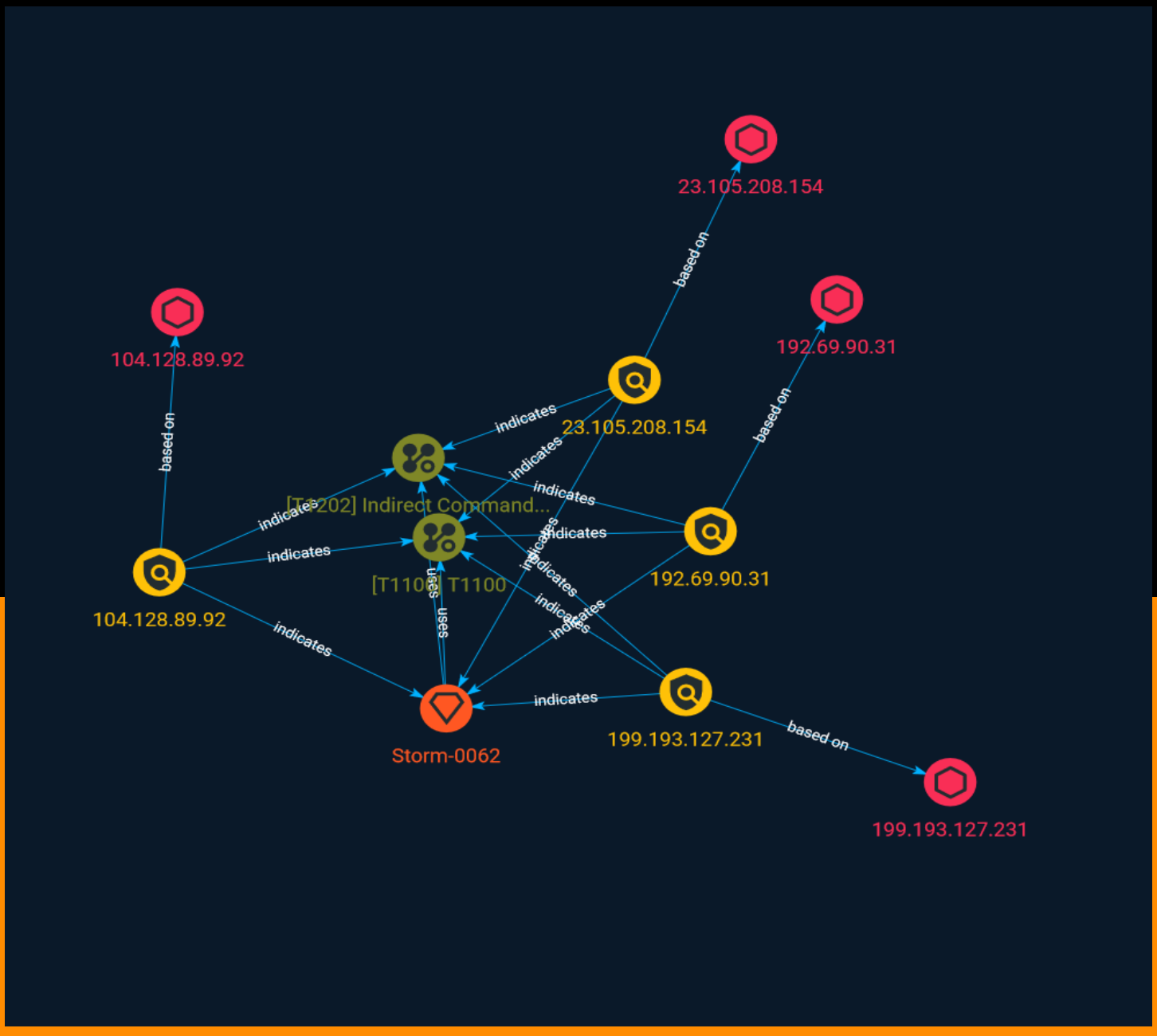

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Atlassian is investigating reports from a few customers regarding the potential exploitation of an undisclosed vulnerability in publicly accessible Confluence Data Center and Server instances, allowing unauthorized access and the creation of administrator accounts.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
T1100
ID
T1100
Name
Indirect Command Execution
ID
T1202
Description
Adversaries may abuse utilities that allow for command execution to bypass security restrictions that limit the use of command-line interpreters. Various Windows utilities may be used to execute commands, possibly without invoking [cmd](https://attack.mitre.org/software/S0106). For example, [Forfiles](https://attack.mitre.org/software/S0193), the Program Compatibility Assistant (pcalua.exe), components of the Windows Subsystem for Linux (WSL), as well as other utilities may invoke the execution of programs and commands from a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), Run window, or via scripts. (Citation: VectorSec ForFiles Aug 2017) (Citation: Evi1cg Forfiles Nov 2017) Adversaries may abuse these features for [Defense Evasion](https://attack.mitre.org/tactics/TA0005), specifically to perform arbitrary execution while subverting detections and/or mitigation controls (such as Group Policy)

that limit/prevent the usage of [cmd](https://attack.mitre.org/software/S0106) or file extensions more commonly associated with malicious payloads.

Indicator

Name

23.105.208.154

Description

ISP: IT7 Networks Inc **OS:** None ---------- Hostnames: - 23.105.208.154.16clouds.com ---------- Domains: - 16clouds.com ---------- Services: **443:** ``` HTTP/1.1 200 OK Set-Cookie: webvpncontext=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; Secure Content-Type: text/xml Content-Length: 306 X-Transcend-Version: 1 ``` HEARTBLEED: 2023/09/27 11:07:38 23.105.208.154:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '23.105.208.154']

Name

199.193.127.231

Description

ISP: Fiber Logic Inc. **OS:** None ---------- Hostnames: - 199.193.127.231.16clouds.com ---------- Domains: - 16clouds.com

---------- Services: **443:** ``` HTTP/1.1 200 OK Set-Cookie: webvpncontext=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; Secure Content-Type: text/xml Content-Length: 306 X-Transcend-Version: 1 ``` HEARTBLEED: 2023/10/12 08:26:45 199.193.127.231:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '199.193.127.231']

Name

104.128.89.92

Description

ISP: Fiber Logic Inc. **OS:** None ---------- Hostnames: - 104.128.89.92.16clouds.com ---------- Domains: - 16clouds.com ---------- Services: **443:** ``` HTTP/1.1 200 OK Set-Cookie: webvpncontext=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; Secure Content-Type: text/xml Content-Length: 306 X-Transcend-Version: 1 ``` HEARTBLEED: 2023/10/12 11:08:56 104.128.89.92:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '104.128.89.92']

Name

192.69.90.31

Description

ISP: Fiber Logic Inc. **OS:** None ---------- Hostnames: - 192.69.90.31.16clouds.com ---------- Domains: - 16clouds.com ---------- Services: **443:** ``` HTTP/1.1 200 OK Set-Cookie: webvpncontext=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; Secure Content-Type: text/xml Content-Length: 306 X-Transcend-Version: 1 ``` HEARTBLEED: 2023/09/30 04:36:02 192.69.90.31:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.69.90.31']

Intrusion-Set

Name
Storm-0062

IPv4-Addr

Value
199.193.127.231
23.105.208.154
192.69.90.31
104.128.89.92

External References

- https://otx.alienvault.com/pulse/652832b6f960f3f7421e6da9
- https://cybersecuritynews.com/confluence-zero-day-vulnerability/