Authored by:



TLP:CLEAR
Product ID: AA23-289A
October 16, 2023

Threat Actors Exploit Atlassian Confluence CVE-2023-22515 for Initial Access to Networks

SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and Multi-State Information Sharing and Analysis Center (MS-ISAC) are releasing this joint Cybersecurity Advisory (CSA) in response to the active exploitation of CVE-2023-22515. This recently disclosed vulnerability affects certain versions of Atlassian Confluence Data Center and Server, enabling malicious cyber threat actors to obtain initial access to Confluence instances by creating unauthorized Confluence administrator accounts. Threat actors exploited CVE-2023-22515 as a zero-day to obtain access to victim systems and continue active exploitation post-patch. Atlassian has rated this vulnerability as critical; CISA, FBI, and MS-ISAC expect widespread, continued exploitation due to ease of exploitation.

CISA, FBI, and MS-ISAC strongly encourage network administrators to immediately apply the upgrades provided by Atlassian. CISA, FBI, and MS-ISAC also encourage organizations to hunt for malicious activity on their networks using the detection signatures and indicators of compromise (IOCs) in this CSA. If a potential compromise is detected, organizations should apply the incident response recommendations.

For additional information on upgrade instructions, a complete list of affected product versions, and IOCs, see Atlassian's security advisory for CVE-2023-22515.[1] While Atlassian's advisory provides interim measures to temporarily mitigate known attack vectors, CISA, FBI, and MS-ISAC strongly encourage upgrading to a fixed version or taking servers offline to apply necessary updates.

For a downloadable copy of IOCs, see:

- AA23-289A STIX XML
- AA23-289A STIX JSON

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office or CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. SLTT organizations should report incidents to MS-ISAC (866-787-4722 or SOC@cisecurity.org).

TECHNICAL DETAILS

Overview

CVE-2023-22515 is a critical Broken Access Control vulnerability affecting the following versions of Atlassian Confluence Data Center and Server. **Note:** Atlassian Cloud sites (sites accessed by an atlassian.net domain), including Confluence Data Center and Server versions before 8.0.0, are not affected by this vulnerability.

- 8.0.0
- 8.0.1
- 8.0.2
- 8.0.3
- 8.0.4
- 8.1.0
- 8.1.1
- 8.1.3
- 8.1.4
- 8.2.0
- 8.2.1
- 8.2.2
- 8.2.3
- 8.3.0
- 8.3.1
- 8.3.2
- 8.4.0
- 8.4.1
- 8.4.2
- 8.5.0
- 8.5.1

Unauthenticated remote threat actors can exploit this vulnerability to create unauthorized Confluence administrator accounts and access Confluence instances. More specifically, threat actors can change the Confluence server's configuration to indicate the setup is not complete and use the /setup/setupadministrator.action endpoint to create a new administrator user. The vulnerability is triggered via a request on the unauthenticated /server-info.action endpoint.

Considering the root cause of the vulnerability allows threat actors to modify critical configuration settings, CISA, FBI, and MS-ISAC assess that the threat actors may not be limited to creating new administrator accounts. Open source further indicates an Open Web Application Security Project (OWASP) classification of injection (i.e., CWE-20: Improper Input Validation) is an appropriate description.[2] Atlassian released a patch on October 4, 2023, and confirmed that threat actors exploited CVE-2023-22515 as a zero-day—a previously unidentified vulnerability.[1]

On October 5, 2023, CISA added this vulnerability to its Known Exploited Vulnerabilities Catalog based on evidence of active exploitation. Due to the ease of exploitation, CISA, FBI, and MS-ISAC expect to see widespread exploitation of unpatched Confluence instances in government and private networks.

Post-Exploitation: Exfiltration of Data

Post-exploitation exfiltration of data can be executed through of a variety of techniques. A predominant method observed involves the use of cURL—a command line tool used to transfer data to or from a server. An additional data exfiltration technique observed includes use of Rclone [S1040]—a command line tool used to sync data to cloud and file hosting services such as Amazon Web Services and China-based UCloud Information Technology Limited. **Note:** This does not preclude the effectiveness of alternate methods, but highlights methods observed to date. Threat actors were observed using Rclone to either upload a configuration file to victim infrastructure or enter

cloud storage credentials via the command line. Example configuration file templates are listed in the following Figures 1 and 2, which are populated with the credentials of the exfiltration point:

Figure 1

```
[s3]
type =
env_auth =
access_key_id =
secret_access_key =
region =
endpoint =
location_constraint =
acl =
server_side_encryption =
storage_class =
```

Figure 2

```
[minio]
type =
provider =
env_auth =
access_key_id =
secret_access_key =
endpoint =
acl =
```

The following User-Agent strings were observed in request headers. **Note:** As additional threat actors begin to use this CVE due to the availability of publicly posted proof-of-concept code, an increasing variation in User-Agent strings is expected.

- `Python-requests/2.27.1`
- `curl/7.88.1`

Indicators of Compromise

Disclaimer: Organizations are recommended to investigate or vet these IP addresses prior to taking action, such as blocking.

The following IP addresses were obtained from FBI investigations as of October 2023 and observed conducting data exfiltration:

- `170.106.106[.]16`
- `43.130.1[.]222`
- `152.32.207[.]23`
- `199.19.110[.]14`
- `95.217.6[.]16` (**Note:** This is the official rclone.org website)

Additional IP addresses observed sending related exploit traffic have been shared by Microsoft.[3]

DETECTION METHODS

Network defenders are encouraged to review and deploy Proofpoint's Emerging Threat signatures. See Ruleset Update Summary - 2023/10/12 - v10438.[4]

Network defenders are also encouraged to aggregate application and server-level logging from Confluence servers to a logically separated log search and alerting system, as well as configure alerts for signs of exploitation (as detailed in Atlassian's security advisory).

INCIDENT RESPONSE

Organizations are encouraged to review all affected Confluence instances for evidence of compromise, as outlined by Atlassian.[1] If compromise is suspected or detected, organizations should assume that threat actors hold full administrative access and can perform any number of unfettered actions—these include but are not limited to exfiltration of content and system credentials, as well as installation of malicious plugins.

If a potential compromise is detected, organizations should:

1. Collect and review artifacts such as running processes/services, unusual authentications, and recent network connections.
    a. **Note:** Upgrading to fixed versions, as well as removing malicious administrator accounts may not fully mitigate risk considering threat actors may have established additional persistence mechanisms.
    b. Search and audit logs from Confluence servers for attempted exploitation.[2]
2. Quarantine and take offline potentially affected hosts.
3. Provision new account credentials.
4. Reimage compromised hosts.
5. Report the compromise to CISA via CISA's 24/7 Operations Center (report@cisa.gov or 888-282-0870). The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or IC3.gov. State, local, tribal, and territorial governments should report incidents to the MS-ISAC (SOC@cisecurity.org or 866-787-4722).

MITIGATIONS

As of October 10, 2023, proof-of-concept exploits for CVE-2023-22515 have been observed in open source publications.[5] While there are immediate concerns such as increased risk of exploitation and the potential integration into malware toolkits, the availability of a proof-of-concept presents an array of security and operational challenges that extend beyond these immediate issues. Immediate action is strongly advised to address the potential risks associated with this development.

CISA, FBI, and MS-ISAC recommend taking immediate action to address the potential associated risks and encourage organizations to:

> These mitigations apply to all organizations using non-cloud Atlassian Confluence Data Center and Server software. CISA, FBI, and MS-ISAC recommend that software manufacturers incorporate secure by design and default principles and tactics into their software development practices to reduce the prevalence of Broken Access Control vulnerabilities, thus strengthening the secure posture for their customers.
>
> For more information on secure by design, see CISA's Secure by Design and Default webpage and joint guide.

- **Immediately upgrade to fixed versions.** See Atlassian's upgrading instructions[6] for more information. If unable to immediately apply upgrades, **restrict untrusted network access until feasible**. Malicious cyber threat actors who exploit the affected instance can escalate to administrative privileges.
- **Follow best cybersecurity practices in your production and enterprise environments.** While not observed in this instance of exploitation, mandating phishing-resistant multifactor authentication (MFA) for all staff and services can make it more difficult for threat actors to gain access to networks and information systems. For additional best practices, see:
  - **CISA's Cross-Sector Cybersecurity Performance Goals (CPGs).** The CPGs, developed by CISA and the National Institute of Standards and Technology (NIST), are a prioritized subset of IT and OT security practices that can meaningfully reduce the likelihood and impact of known cyber risks and common tactics, techniques, and procedures (TTPs). Because the CPGs are a subset of best practices, CISA recommends software manufacturers implement a comprehensive information security program based on a recognized framework, such as the NIST Cybersecurity Framework (CSF).
  - **Center for Internet Security's (CIS) Critical Security Controls.** The CIS Critical Security Controls are a prescriptive, prioritized, and simplified set of best practices that organizations can use to strengthen cybersecurity posture and protect against cyber incidents.

RESOURCES

- NIST: CVE-2023-22515
- MITRE: CWE-20 - Improper Input Validation
- CISA: Known Exploited Vulnerabilities Catalog

- MITRE Software: Rclone
- CISA: Secure by Design and Default
- CISA: Phishing-Resistant MFA
- CISA: Cross-Sector Cybersecurity Performance Goals
- CIS: Critical Security Controls

REFERENCES

[1] Atlassian: CVE-2023-22515 - Broken Access Control Vulnerability in Confluence Data Center and Server
[2] Rapid7: CVE-2023-22515 Analysis
[3] Microsoft: CVE-2023-22515 Exploit IP Addresses
[4] Proofpoint: Emerging Threats Rulesets
[5] Confluence CVE-2023-22515 Proof of Concept - vulhub
[6] Atlassian Support: Upgrading Confluence

DISCLAIMER

VERSION HISTORY

October 16, 2023: Initial version.