

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## **Atlassian Confluence Zero-Day Actively Exploited in the Wild**

Date of Publication  
October 5, 2023

Last Update Date  
October 18, 2023

Admiralty Code  
A1

TA Number  
TA2023397

# Summary




**First Seen:** October 4, 2023

**Affected Products:** Confluence Data Center and Confluence Server

**Actor:** Storm-0062 (aka DarkShadow, Oro0lxy)

**Impact:** A critical zero-day flaw, identified as CVE-2023-22515, affecting Confluence Data Center and Server instances is being actively exploited. This remotely exploitable vulnerability enables external attackers to create unauthorized Confluence administrator accounts and gain access to Confluence servers.

## CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-22515	Atlassian Confluence Broken Access Control Vulnerability	Confluence Data Center and Confluence Server			

# Vulnerability Details

## #1

CVE-2023-22515 is a critical Broken Access Control vulnerability that affects on-premise Atlassian Confluence Data Center and Server products. This vulnerability poses a significant security risk because it allows a remote, unauthenticated attacker to compromise the affected system. An attacker can exploit this vulnerability by sending specially crafted requests to the server, which can result in the creation of unauthorized administrative accounts and unauthorized access to the system.

## #2

This vulnerability allows threat actors to change the Confluence server's configuration to indicate that the setup is not complete. They can then use the `"/setup/setupadministrator.action"` endpoint to create a new administrator user. The vulnerability appears to be triggered via a request on the unauthenticated `"/server-info.action"` endpoint.

## #3

Instances of Atlassian Confluence that are accessible on the public internet are at heightened risk, with malicious actors exploiting this flaw without requiring any login credentials. Multiple threat actors have been detected conducting data exfiltration using diverse techniques, including cURL, Rclone, and leveraging cloud storage to stage exfiltrated files.

## #4

To effectively mitigate the risk associated with the CVE-2023-22515 vulnerability in Confluence Server or Data Center, it is strongly advised to upgrade to the fixed versions that Atlassian has provided. It's worth noting that versions prior to 8.0.0 are not impacted by this vulnerability. If, for any reason, an immediate upgrade is not possible, Atlassian provides mitigation guidance that should be followed.


## #5


Atlassian recently addressed a range of vulnerabilities in their products, spanning from Remote Code Execution to Denial-of-Service vulnerabilities. [CVE-2023-22512](#) impacts Confluence Server, where an unauthenticated attacker can trigger a Denial of Service.


## Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-22515	Confluence Data Center and Confluence Server Versions- 8.0.x, 8.1.x, 8.2.x, 8.3.0, 8.3.1, 8.3.2, 8.4.0, 8.4.1, 8.4.2, 8.5.0, 8.5.1	cpe:2.3:a:atlassian:confluence_server_and_data_center:*:*:*:*:*	CWE-284

## Recommendations

 **Apply Patch:** Install the security patch provided by Atlassian to address the CVE-2023-22515 vulnerability. These patches shall close the security gap that allows attackers to exploit the vulnerability.

 **System Event Monitoring:** Utilize automated systems for System Event Monitoring, ensuring constant surveillance of account creation or other critical Confluence system activities in real time. The monitoring platform should be capable of instantly notifying administrators or security teams upon detecting any suspicious activities.

 **Limit Service Exposure:** Consider limiting service exposure to specific networks, such as VPN or Intranet, to reduce the attack surface and minimize system exposure to potential threats. Additionally, restrict access to /setup/\* endpoints on Confluence instances to effectively block known attack vectors.

## Potential MITRE ATT&CK TTPs

<b><u>TA0001</u></b> Initial Access	<b><u>TA0042</u></b> Resource Development	<b><u>TA0004</u></b> Privilege Escalation	<b><u>TA0003</u></b> Persistence
<b><u>TA0010</u></b> Exfiltration	<b><u>T1068</u></b> Exploitation for Privilege Escalation	<b><u>T1588</u></b> Obtain Capabilities	<b><u>T1588.006</u></b> Vulnerabilities
<b><u>T1190</u></b> Exploit Public-Facing Application	<b><u>T1078</u></b> Valid Accounts	<b><u>T1136</u></b> Create Account	<b><u>T1567</u></b> Exfiltration Over Web Service
<b><u>T1567.002</u></b> Exfiltration to Cloud Storage			

## Indicators of Compromise (IOCs)

TYPE	VALUE
<b>IPv4</b>	170.106.106[.]16, 43.130.1[.]222, 152.32.207[.]23, 199.19.110[.]14, 192.69.90[.]31, 104.128.89[.]92, 23.105.208[.]154, 199.193.127[.]231

## Patch Details

It is recommended to update to the latest version of Atlassian Confluence products which addresses the CVE-2023-22515. Atlassian have fixed this vulnerability in following versions.

8.3.3 or later

8.4.3 or later

8.5.2 (Long Term Support release) or later

Patch Link:

<https://www.atlassian.com/software/confluence/download-archives>

Atlassian has also provided mitigation steps to decrease the likelihood of exploitation. Refer to the following link for detailed mitigation instructions.

Mitigation Link:

<https://confluence.atlassian.com/security/cve-2023-22515-privilege-escalation-vulnerability-in-confluence-data-center-and-server-1295682276.html>

## References

<https://confluence.atlassian.com/security/cve-2023-22515-privilege-escalation-vulnerability-in-confluence-data-center-and-server-1295682276.html>

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-289a>

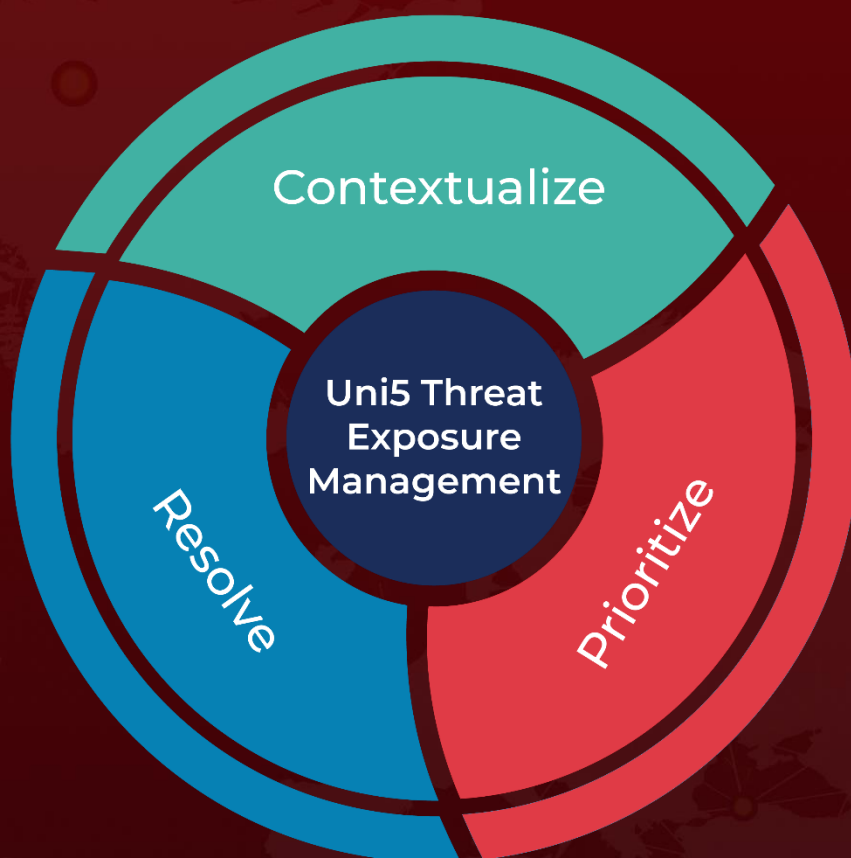
<https://www.hivepro.com/critical-security-vulnerabilities-discovered-in-atlassian-products/>

<https://twitter.com/MsftSecIntel/status/1711871732644970856>

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**October 5, 2023 • 6:50 AM**

© 2023 All Rights are Reserved by Hive Pro®



More at [www.hivepro.com](http://www.hivepro.com)