

HiveForce Labs

# THREAT ADVISORY



## VULNERABILITY REPORT

### **Atlassian's Latest Critical Confluence Flaw Poses Risk of Data Loss**

Date of Publication

November 01, 2023

Last Update Date

November 16, 2023

Admiralty Code

A1

TA Number

TA2023442




# Summary

**First Discovered:** October 31, 2023

**Affected Product:** Confluence Data Center, Confluence Server

**Impact:** A critical vulnerability identified in Atlassian as CVE-2023-22518 which pertains to be an improper authorization issue in Confluence Data Center and Server, exploiting the vulnerability allows unauthorized users to reset and create a Confluence instance administrator account. The Cerber ransomware group has been observed exploiting this flaw.

## CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-22518	Atlassian Confluence Improper Authorization Vulnerability	Confluence Data Center, Confluence Server			

# Vulnerability Details

## #1

CVE-2023-22518 is a critical security vulnerability that Atlassian has identified in Confluence Data Center and Server. It involves an improper authorization issue that, if successfully exploited has the potential to result in significant data loss.

## #2

The vulnerability CVE-2023-22518 which can be exploited by a remote, unauthenticated attacker by sending specially crafted requests to the server, an attacker can bypass the authorization process and gain unauthorized access, potentially leading to data modification on the system.

## #3

In November, the Cerber ransomware has been observed utilizing the CVE-2023-22518 vulnerability as part of its attack routine. In this infection chain, the threat actor gains access through the vulnerability, executing an encoded PowerShell command to download and execute a remote payload.

## #4

The PowerShell script downloads a malicious text file from a command-and-control server, revealing the Cerber ransomware payload. The script executes the decoded payload, encrypts files, and drops a ransom note. Multiple Linux bash files were also downloaded from the same IP address.


## #5


System administrators are strongly advised to take immediate action and upgrade to the fixed version of Confluence Data Center and Server to address this critical vulnerability (CVE-2023-22518). It's essential to act swiftly, as previously discovered vulnerability in the software [CVE-2023-22515](#), have also been exploited by threat actors in the past.


## Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-22518	Confluence Data Center and Server 6.0.1 - 8.6.0	cpe:2.3:a:atlassian:confluence_server_and_data_center:8.6.0:*:*:*:*:*	CWE-285

## Recommendations

 **Apply Patch:** Install the security patch provided by Atlassian to address the CVE-2023-22518 vulnerability. This patch closes the security gap that allows attackers to exploit the vulnerability.

 **Least Privilege:** Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.

 **Conduct Regular Backup:** Establish routine backups for all assets, ensuring they receive proper protection. Implement the 3-2-1-1 backup principle and deploy dedicated tools to guarantee backup integrity and availability.

# Potential MITRE ATT&CK TTPs

<b><u>TA0042</u></b> Resource Development	<b><u>TA0001</u></b> Initial Access	<b><u>TA0002</u></b> Execution	<b><u>TA0004</u></b> Privilege Escalation
<b><u>TA0011</u></b> Command and Control	<b><u>TA0040</u></b> Impact	<b><u>T1190</u></b> Exploit Public-Facing Application	<b><u>T1588</u></b> Obtain Capabilities
<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1485</u></b> Data Destruction	<b><u>T1059</u></b> Command and Scripting Interpreter	<b><u>T1059.001</u></b> PowerShell
<b><u>T1078</u></b> Valid Accounts			

## Indicators of Compromise (IOCs)

TYPE	VALUE
<b>IP</b>	193.187.172[.]73
<b>URL</b>	hxxp://193.176[.]179[.]41/tmp.37

## Patch Link

It is recommended to update to the latest version of Atlassian Confluence Data Center and Server which addresses the CVE-2023-22518. Atlassian have fixed this vulnerability in following versions.

7.19.16 or later

8.3.4 or later

8.4.4 or later

8.5.3 or later

8.6.1 or later

Patch Link:

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

## References

<https://confluence.atlassian.com/security/cve-2023-22518-improper-authorization-vulnerability-in-confluence-data-center-and-confluence-server-1311473907.html>

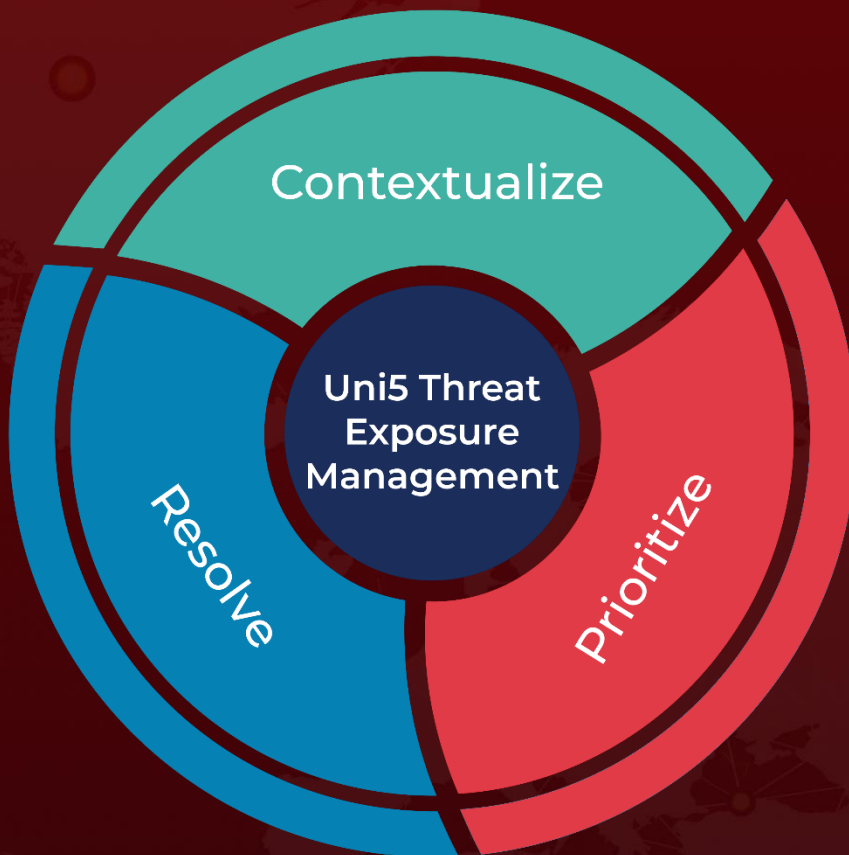
<https://www.hivepro.com/atlassian-confluence-zero-day-actively-exploited-in-the-wild/>

[https://www.trendmicro.com/en\\_us/research/23/k/cerber-ransomware-exploits-cve-2023-22518.html](https://www.trendmicro.com/en_us/research/23/k/cerber-ransomware-exploits-cve-2023-22518.html)

# 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

**November 01, 2023 • 4:30 AM**

© 2023 All Rights are Reserved by HivePro®



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