



PROFILE

CVE-2022-26134

ZEROFOX INTELLIGENCE

P-2023-01-06a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Common Vulnerabilities & Exposures

Created on: December 29, 2022

January 6, 2023



PROFILE: CVE-2022-26134

P-2023-01-06a

TLP:CLEAR

Intelligence Cut-off: 12:00 PM (EST) on January 6, 2023

First Observed: June 7, 2022

CVE Dictionary Entry: CVE-2022-26134

NVD Published Date: June 3, 2022

NVD Last Modified: June 30, 2022

Severity: CRITICAL

Base Score: 9.8

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Metasploit Available: Yes

Current Description

CVE-2022-26134 is an Open Graph Navigation Language (OGNL) injection vulnerability that allows an unauthenticated attacker to execute arbitrary code on affected versions of an Atlassian Confluence server or data center instance. The affected versions are from 1.3.0 before 7.4.17, from 7.13.0 before 7.13.7, from 7.14.0 before 7.14.3, from 7.15.0 before 7.15.2, from 7.16.0 before 7.16.4, from 7.17.0 before 7.17.4, and from 7.18.0 before 7.18.1.

Risk

CVE-2022-26134 provides threat actors with the ability to remotely execute arbitrary commands without authentication. Successful exploitation of a Confluence server leveraging this vulnerability could provide threat actors a foothold within a corporate network. Given that the vulnerable application is a Confluence application, and Confluence is often leveraged to house company-sensitive information, a compromise within this application can have severe consequences.

ZeroFox assesses this vulnerability to have a High risk rating, since it is quite easy to implement and successfully exploit. The presence of a Metasploit module on GitHub using this OGNL injection allows for anyone to scan for and exploit it, making it likely that threat actors will leverage this vulnerability.



Known Affected Software Configurations

Configuration	Common Platform Enumeration
1	cpe:2.3:a:atlassian:confluence_data_center:*****
1	cpe:2.3:a:atlassian:confluence_data_center:*****
1	cpe:2.3:a:atlassian:confluence_data_center:*****
1	cpe:2.3:a:atlassian:confluence_data_center:*****
1	cpe:2.3:a:atlassian:confluence_data_center:*****
1	cpe:2.3:a:atlassian:confluence_data_center:*****
1	cpe:2.3:a:atlassian:confluence_data_center:7.18.0:*****
1	cpe:2.3:a:atlassian:confluence_server:*****
1	cpe:2.3:a:atlassian:confluence_server:*****
1	cpe:2.3:a:atlassian:confluence_server:*****
1	cpe:2.3:a:atlassian:confluence_server:*****
1	cpe:2.3:a:atlassian:confluence_server:*****
1	cpe:2.3:a:atlassian:confluence_server:*****
1	cpe:2.3:a:atlassian:confluence_server:7.18.0:*****

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ("Injection")	NIST



Vulnerability Analysis

CVE-2022-26134 is a Remote Code Execution (RCE) within Atlassian Confluence Server. The first widely-reported proof-of-concept leveraging this vulnerability was provided on June 7, 2022.¹ A Metasploit module leveraging this vulnerability was subsequently uploaded to GitHub.

The simplicity of this exploit, along with an available Metasploit module, allows for threat actors to scan for this vulnerability easily. Even months after the public release of this exploit, threat actors are still looking for vulnerable systems. This active interest is shown in Figure 1; GreyNoise[.]io detected 522 unique IP addresses attempting to exploit CVE-2022-26134 throughout the month of December 2022.



Figure 1. Unique IP scanning for CVE-2022-26134 over time

Source:

[https://viz.greynoise\[.\]io/tag/atlassian-confluence-server-cve-2022-26134-ognl-injection-attempt?days=30](https://viz.greynoise[.]io/tag/atlassian-confluence-server-cve-2022-26134-ognl-injection-attempt?days=30)

CVE-2022-26134 takes advantage of an OGNL injection within the Uniform Resource Identifier (URI) of the Confluence application. An OGNL injection is a subclass of an Expression Language (EL) injection in which a string that is submitted by an attacker is eventually interpreted by an EL Interpreter. In this case, the exploit can abuse this

¹

[https://packetstormsecurity\[.\]com/files/167430/Confluence-OGNL-Injection-Remote-Code-Execution.html](https://packetstormsecurity[.]com/files/167430/Confluence-OGNL-Injection-Remote-Code-Execution.html)



OGNL injection to gain access to `java.lang.Runtime.getRuntime().exec()`. This Java function allows for the execution of operating system commands.

Recommendations

Since the advisory release date of June 3, 2022, for CVE-2022-26134, Atlassian has released a patch for all affected versions. ZeroFox Intelligence recommends updating Confluence applications to the latest versions. If updating is not immediately possible, put the Confluence application behind a VPN, limiting its exposure to the internet. ZeroFox also recommends installing and configuring Filebeat to ingest Confluence logs. On an Ubuntu Server Installation, the logs can be located within the `/opt/atlassian/confluence/logs/` folder.



Appendix 1: Indicators of Compromise (Sigma Rules)

```
title: CVE-2022-26134
id: f56144bd-fb1e-43e6-ab07-bf0866840052
description: Sigma detection rule for an exploit attempt leveraging
CVE-2022-26134 against a vulnerable confluence application installed on
a ubuntu server. This rule attempts to match on an OGNL String that
contains Java Bean that leads to OS Command Injection.
status: experimental
date: 2023/1/05
modified: 2023/1/05
author: ZeroFox
tags:
  - mitre.T1190
  - mitre.T1059
  - attack.InitialAccess
  - attack.Execution
references:
  - https://nvd.nist.gov/vuln/detail/cve-2022-26134
  -
http://packetstormsecurity.com/files/167430/Confluence-OGNL-Injection-Remote-Code-Execution.html
-
http://packetstormsecurity.com/files/167431/Through-The-Wire-CVE-2022-26134-Confluence-Proof-Of-Concept.html
-
http://packetstormsecurity.com/files/167432/Confluence-OGNL-Injection-Proof-Of-Concept.html
-
http://packetstormsecurity.com/files/167449/Atlassian-Confluence-Namespace-OGNL-Injection.html
-
https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html
  - https://jira.atlassian.com/browse/CONFSERVER-79016
logsource:
  product: linux
detection:
  logfile:
    - log.file.path: '*conf_access_log*.log'
  uppercase:
    event.original:
      - '%24%7B*java.lang.Runtime.getRuntime%28%29.exec*%7D*' #matching
on ${ ... Java bean ... }
  lowercase:
    event.original:
      - '%24%7b*java.lang.Runtime.getRuntime%28%29.exec*%7d*' #matching
on ${ ... Java bean ... }
  condition: logfile and (uppercase or lowercase)
level: critical
```

Figure 2. Sigma Rule to detect CVE-2022-26134

Source: ZeroFox Intelligence Collections



Appendix 2: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.