CVE-2023-22527 Atlassian Confluence Data Center and Server Template Injection Vulnerability

On January 16, 2024, Atlassian disclosed a security vulnerability allowing remote code execution (RCE) affecting both Confluence Data Center and Confluence Server. This security flaw, identified as CVE-2023-22527, is an OGNL injection vulnerability with a CVSS score of 10 (Critical).

Due to its critical severity and allowing unauthenticated RCE, this vulnerability will attract significant interest from both security researchers and threat actors.

CVSS score is as follows:

- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H ⇒ Base Score: 10.0 CRITICAL
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H ⇒ Base Score: 9.8 CRITICAL

Affected Versions

According to the disclosure made by Atlassian, the CVE-2023-22527 vulnerability affects the following versions: [1]

Product	Affected Versions
Confluence Data Center and Server	• 8.0.x • 8.1.x • 8.2.x • 8.3.x • 8.4.x • 8.5.0 - 8.5.3

Attack Models and Potential Impact

The exploitation of CVE-2023-22527 can pose serious security risks on affected systems.

Attack Models:

- CVE-2023-22527 allows attackers to gain unauthorized access to affected Atlassian Confluence systems via template injection.
- Attackers can inject malicious code into the server using template injection and abuse system resources.

Potential Impact:

- Attackers can gain access to sensitive information and execute malicious software, such as ransomware, on systems.
- Attackers can obtain unauthorized access to the server and access sensitive data or take control of the server to operate as they please.

The exploitation of CVE-2023-22527 can pose serious security risks on affected systems. Attackers can exploit this vulnerability to gain unauthorized access and manipulate the system as they wish. Potential impacts include data leakage, data loss, system crashes, and ransomware attacks. Such attacks can lead to serious consequences such as business continuity and reputation loss.

Indicators of Compromise (IOCs)

According to ShadowServer's Twitter post, more than 600 IP addresses were observed attempting thousands of exploits using CVE-2023-22527. Additionally, various sources such as GreyNoise, ShadowServer, SANS Internet Storm Center (ISC), and The DFIR Report [1, 2] have confirmed observations of wild exploitation attempts using CVE-2023-22527. Some IoC lists [1], [2], [3], [4] also support this validation.

- **IP Addresses:**

1. 23.227.194[.]230
2. 46.232.121[.]223
3. 209.222.10[.]213
4. 104.28.245[.]205
5. 107.167.2[.]220
6. 134.122.186[.]223
7. 140.82.32[.]34
8. 141.164.54[.]191
9. 144.24.38[.]152
10. 149.102.70[.]165
11. 149.104.23[.]176
12. 156.234.193[.]62
13. 188.192.12[.]36
14. 195.211.124[.]184
15. 159.223.87[.]79
16. 20.205.116[.]139
17. 221.216.117[.]91
18. 31.41.221[.]123
19. 38.150.12[.]131
20. 38.181.44[.]171
21. 38.6.173[.]11
22. 52.192.172[.]33
23. 157.230.218[.]201
24. 192.46.208[.]206
25. 198.50.168[.]189
26. 43.129.184[.]65
27. 64.227.149[.]86
28. 39.144.10[.]102
29. 42.2.227[.]212
30. 43.140.203[.]2
31. 43.248.103[.]141
32. 45.77.220[.]169
33. 45.77.98[.]55
34. 65.154.226[.]169
35. 66.154.106[.]13
36. 67.181.73[.]197
37. 91.203.134[.]122
38. 91.216.169[.]56
39. 45.61.137[.]90
40. 193.176.179[.]41
41. 193.43.72[.]11
42. 45.145.6[.]112
43. 38.180.75[.]124
44. 38.150.12[.]144
45. 186.117.138[.]210
46. 158.247.248[.]34
47. 117.188.118[.]53
48. 103.73.66[.]37
49. 1.53.255[.]131
50. 1.55.80[.]91
51. 23.94.214[.]119

Domain Names:

- j3qxmk6g5sk3zw62i2yhjnwmhm55rfz47fdyfkhaithlpelfjdokdxad[.]onion
- redacted[.]oast[.]site
- redacted[.]oast[.]pro
- redacted[.]oast[.]live

File Hashes:

- MD5: 81b760d4057c7c704f18c3f6b3e6b2c4
- SHA256: 4ed46b98d047f5ed26553c6f4fded7209933ca9632b998d265870e3557a5cdfe
- SHA1=820498a4ca6b28089321a524a312530f032d9d5b,
- SHA1=ac9ee98d9d24744efdf7989ad6d4a937431cef8b,
- SHA1=c0fb9e3903102430014358736f5cc68775a71dd5,
- SHA1=f9c0c07f38706f2798063c58ba983380d2311112,
- SHA1=1ef4a1f20b17a58a435f6aa6c57980bb2f22bec6

Conclusion and Recommendation

The template injection threat posed by CVE-2023-22527 highlights significant security risks for Atlassian Confluence users. It is important to promptly update affected systems and take necessary precautions.

Latest versions:

- Confluence Data Center and Server - 8.5.4 (LTS)
- Confluence Data Center - 8.6.0 or higher (Data Center only) and 8.7.1 or higher (Data Center only)

REFERENCES

Picus Security. (January 23, 2024). CVE-2023-22527: Another OGNL Injection Leads to RCE in Atlassian Confluence. Retrieved from https://www.picussecurity.com/resource/blog/cve-2023-22527-another-ognl-injection-leads-to-rce-in-atlassian-confluence

SOC Prime. (January 23, 2024). CVE-2023-22527 Detection: Maximum Severity RCE Vulnerability in Atlassian's Confluence Server and Data Center Exploited in the Wild. Retrieved from https://socprime.com/blog/cve-2023-22527-detection-maximum-severity-rce-vulnerability-in-atlassians-confluence-server-and-data-center-exploited-in-the-wild/

Arctic Wolf. (January 23, 2024). Exploitation of Confluence Server Vulnerability CVE-2023-22527 Leading to C3RB3R Ransomware. Retrieved from https://arcticwolf.com/resources/blog/confluence-cve-2023-22527-leading-to-c3rb3r-ransomware/

Tenable .(January 23, 2024). CVE-2023-22527: Atlassian Confluence Data Center and Server Template Injection Exploited in the Wild. Retrieved from https://www.tenable.com/blog/cve-2023-22527-atlassian-confluence-data-center-and-server-template-injection-exploited-in-the

Hive Pro. (January 24, 2024) Critical RCE Flaw in Atlassian Confluence Sparks Active Exploitation Retrieved from https://www.hivepro.com/wp-content/uploads/2024/01/Critical-RCE-Flaw-in-Atlassian-Confluence-Sparks-Active-Exploitation_TA2024030.pdf