Observed Exploitation of Atlassian Confluence CVE-2023-22518

Date: 19th April 2024 | Severity: High

Summary

Atlassian Confluence Data Center and Server contain an improper authorization vulnerability that can result in significant data loss when exploited by an unauthenticated attacker. There is no impact on confidentiality since the attacker cannot exfiltrate any data.

Attack Vectors

All versions of Confluence Data Center and Server are affected by this unexploited vulnerability. This Improper Authorization vulnerability allows an unauthenticated attacker to reset Confluence and create a Confluence instance administrator account. Using this account, an attacker can then perform all administrative actions that are available to Confluence instance administrator leading to - but not limited to - full loss of confidentiality, integrity and availability.

Indicator of compromise

INDICATOR TYPE	INDICATORS
CVE ID	2CVE-2023-22518
Domain	j3qxmk6g5sk3zw62i2yhjnwmhm55rfz47fdyfkhaithlpelfjdokdxad.onion webhook.site telete.in
Url	http://128.199.118.202/tmp.sh.2p

File Hash	43b84a6ad0cd2ee1d40cc93a17785e7bc01e946e4176a98a74aa98a74e50c730 02f3f8d14acf7c5d5c026a449200bcbe0576ea66870d79e174e5f2349062bd-ca dfa17e1496d92dfc4b2d29aad3e3b5a5ac4ef6a0ee469281ee86c2ad2ff1691f 08ce2dac33264f90d5ad8d89bbe56ad0346fc32854a184ed23b15c1cfac81a63 04e8daa018dca72480648ab5a8c9de4491921e3250fa5a1cdf9ddea234dd1d81 2b921630e3606ceded2567dd7c2665ff59d3894e8f17b0c4c515cfcfea9281f6 ad3db6873ee057313747e045dd8524d25d5e4e2788adb4560611a4cbf4b70f9f 03f719cc549c461a71c1d8f7889792d2f54ef571f8082abd8cdb00613d913d0e dc0ce179f739c3294acca308e2baa9b4 6989058fd659095de56f66b4399d58b-919ceb66a93d1a9fd2db79efac8741280 06fbbf4aa44810136e505633664deb2f-f4e69e738b0c8f1cffe7ecbe452fba58 4c41f045065a4fca849d0b189024c9aa734cc7e-0a7805e5df8c9be222edaccb2
IP	84.17.48.94 | 193.176.179.41 | 45.145.6.112 | 45.79.19.196 | 144.76.136.153 96.126.123.244 | 45.33.2.79 | 216.158.226.206 | 27.1.1.34 | 193.43.72.11 162.243.175.63 | 212.237.5.209

Recommendation

Product	**Affected Version**
Confluence Data Center and Server	All versions are affected

Atlassian recommends that you patch each of your affected versions.

Reference Links

- https://www.cvedetails.com/cve/CVE-2023-22518/?q=CVE-2023-22518
- https://confluence.atlassian.com/security/cve-2023-22518-improper-authorization-vulnerability-in-confluence-data-center-and-server-1311473907.html
- https://www.rapid7.com/blog/post/2023/11/06/etr-rapid7-observed-exploitation-of-atlassian-confluence-cve-2023-22518/