



| Flash |

Disclosure of Critical Atlassian Confluence Vulnerability

F-2024-01-17a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Vulnerability Exploitation, Deep Dark
Web & Criminal Underground

January 17, 2024

Scope Note: ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EST) on January 17, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Disclosure of Critical Atlassian Confluence Vulnerability

› Key Findings

- On January 16, 2024, Atlassian issued a security update to patch CVE-2023-22527, a critical remote code execution flaw in Confluence Data Center and Confluence Server. The exploit impacts all Confluence Data Center and Server 8 versions released prior to December 5, 2023.
- Atlassian's security update is part of a wider bulletin affecting a total of 29 vulnerabilities across several of its products.
- Atlassian Confluence exploits have a history of being widely-exploited by threat actors. While no proof of active exploitation in the wild has yet been identified, threat actors will very likely leverage this exploit against unpatched networks in the short term.
- ZeroFox urges users to ensure networks are patched with the latest Atlassian software updates.

| Details

On January 16, 2024, Atlassian issued a security update to patch CVE-2023-22527, a critical remote code execution flaw in Confluence Data Center and Confluence Server.

CVE-2023-22527 is a template injection vulnerability that enables unauthenticated, remote threat actors to execute malicious code on vulnerable networks. Successful exploitation of the vulnerability can facilitate data theft, deployment of malicious payloads such as ransomware, and lateral movement.

- The vulnerability has been assigned the maximum critical CVSS score of 10 out of 10.
- The exploit impacts all Confluence Data Center and Server 8 versions released prior to December 5, 2023, including versions 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x, and 8.5.0 through 8.5.3.
- End-of-life instances (versions 8.4.5 and before) are also affected and will not receive patches.

There are currently no known workarounds. Users are urged to implement the patch by updating to the latest versions immediately, regardless of whether instances are exposed to the Internet.

- Confluence Data Center and Server users should update to v8.5.5 (LTS).
- Confluence Data Center (only) users should update to v8.7.2.
- Cloud instances are unaffected.

Atlassian's security update is part of a wider bulletin affecting a total of 29 vulnerabilities across several of its products. A full list of vulnerabilities and affected versions can be found in Appendix A.

Atlassian Confluence exploits have a history of being widely-exploited by threat actors, due to its broad dispersion amongst organizations and their supply chains, deep embedment in networking environments, and a very likely high number of unpatched networks.

- Although no overt claims of active exploitation in the wild have yet been identified in non-private deep and dark web forums, there is a roughly even chance that threat actors are already exploiting unpatched servers.
- Threat actors will very likely leverage this exploit against unpatched networks in the short term.

| Recommendations

- Ensure networks are patched with the latest Atlassian Confluence Data Center and Server versions, as described above.
 - [hXXps://confluence.atlassian\[.\]com/security/cve-2023-22527-rce-remote-code-execution-vulnerability-in-confluence-data-center-and-confluence-server-1333990257.html](https://confluence.atlassian[.]com/security/cve-2023-22527-rce-remote-code-execution-vulnerability-in-confluence-data-center-and-confluence-server-1333990257.html)
 - [hXXps://confluence.atlassian\[.\]com/security/security-bulletin-january-16-2024-1333335615.html](https://confluence.atlassian[.]com/security/security-bulletin-january-16-2024-1333335615.html)
- Ensure a thorough understanding of organizational technology stacks, including those of operating partners.
- Consistently monitor for security patch releases impacting these products, and deploy a holistic patch management system to ensure all business IT assets are updated with the latest software as quickly as possible.
- Conduct a thorough assessment of servers and review any relevant activity logs for suspicious behavior.
- Leverage CISA's KEV catalog to prioritize out-of-cycle vulnerability patching.
- Protect endpoint devices with phishing-resistant MFA protocols compliant with FIDO2 or PKI standards.
- Ensure critical data is backed up to secure off-site or cloud servers. Sensitive or proprietary data should be properly compartmentalized, avoiding aggregation or unnecessary accumulation.
- Use the ZeroFox Platform's Intelligence Search capability to investigate vulnerabilities and associated exploits.
- Maintain a clear and comprehensive incident response strategy consisting of business resilience and continuity plans, incident reporting procedures, and key authorities.

Appendix A: Vulnerabilities Addressed in Atlassian's Security Update on January 16, 2024

CVE	Description	Affected Versions	CVSS v3.x ¹	Severity
CVE-2023-22527	Remote Code Execution (RCE) Vulnerability In Confluence Data Center and Confluence Server	All series 8 versions, including 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x, and 8.5.0 through 8.5.3	10	Critical
CVE-2022-42252	org.apache.tomcat:tomcat-coyote Dependency in Jira Software Data Center and Server	All versions including and after 9.4.0	7.5	High
CVE-2020-25649	XML External Entity (XXE) Injection jackson-databind Dependency in Jira Software Data Center and Server	All versions including and after 8.20.0	7.5	High
CVE-2022-44729	Server-side Request Forgery (SSRF) org.apache.xmlgraphics:batik-bridge Dependency in Jira Service Management Data Center and Server	All versions including and after 4.20.0	7.1	High
CVE-2021-40690	Info Disclosure org.apache.santuario:xmlsec Dependency in Crowd Data Center and Server	All versions including and after 3.4.6	7.5	High
CVE-2023-46589	Request Smuggling org.apache.tomcat:tomcat-catalina Dependency in Crowd Data Center and Server	All versions including and after 3.4.6	7.5	High
CVE-2023-3635	Denial of Service (DoS) com.squareup.okio:okio-jvm Dependency in Confluence Data Center and Server	All versions including and after 7.13.0	7.5	High
CVE-2023-22526	RCE in Confluence Data Center and Server	All versions including and after 7.13.0	7.2	High

¹ Analyst note: N/A for CVSS v3.x indicates that a CVSS score/severity for this CVE has not been published yet.

Flash | Disclosure of Critical Atlassian Confluence Vulnerability

F-2024-01-17a

TLP: CLEAR



CVE	Description	Affected Versions	CVSS v3.x ¹	Severity
CVE-2024-21672	RCE in Confluence Data Center and Server	All versions including and after 2.1	8.3	High
CVE-2024-21673	RCE in Confluence Data Center and Server	All versions including and after 1.0.0	8	High
CVE-2024-21674	RCE in Confluence Data Center and Server	All versions including and after 1.0.0	8.6	High
CVE-2023-43642	DoS (Denial of Service) org.xerial.snappy:snappy-java Dependency in Bitbucket Data Center and Server	All versions including and after 7.21.0	7.5	High
CVE-2023-6481	DoS ch.qos.logback:logback-core Dependency in Bitbucket Data Center and Server	All versions including and after 7.21.0	7.5	High
CVE-2023-6378	DoS ch.qos.logback:logback-core Dependency in Bitbucket Data Center and Server	All versions including and after 7.21.0	7.5	High
CVE-2023-46589	Request Smuggling org.apache.tomcat.embed:tomcat-embed-core Dependency in Bitbucket Data Center and Server	All versions including and after 7.21.0	7.5	High
CVE-2023-34455	DoS org.xerial.snappy:snappy-java Dependency in Bitbucket Data Center and Server	All versions including and after 7.21.0	7.5	High
CVE-2023-34454	DoS org.xerial.snappy:snappy-java Dependency in Bitbucket Data Center and Server	All versions including and after 7.21.0	7.5	High
CVE-2023-34453	DoS org.xerial.snappy:snappy-java Dependency in Bitbucket Data Center and Server	All versions including and after 7.21.0	7.5	High
CVE-2023-36478	DoS org.eclipse.jetty:jetty-http	All versions	7.5	High

Flash | Disclosure of Critical Atlassian Confluence Vulnerability

F-2024-01-17a

TLP:CLEAR



CVE	Description	Affected Versions	CVSS v3.x ¹	Severity
	Dependency in Bitbucket Data Center and Server	including and after 8.9.0		
CVE-2023-5072	DoS org.json:json Dependency in Bitbucket Data Center and Server	All versions including and after 7.17.0	7.5	High
CVE-2023-36478	DoS org.eclipse.jetty:jetty-http Dependency in Bamboo Data Center and Server	All versions including and after 9.2.1	7.5	High
CVE-2023-39410	DoS org.apache.avro:avro Dependency in Bamboo Data Center and Server	All versions including and after 9.2.1	7.5	High
CVE-2020-26217	RCE org.jvnet.hudson:xstream Dependency in Bamboo Data Center and Server	All versions including and after 9.2.1	8.8	High
CVE-2017-7957	DoS org.jvnet.hudson:xstream Dependency in Bamboo Data Center and Server	All versions including and after 9.2.1	7.5	High
CVE-2022-4244	Info Disclosure org.codehaus.plexus:plexus-utils Dependency in Bamboo Data Center and Server	All versions including and after 9.2.1	7.5	High
CVE-2018-10054	RCE com.h2database:h2 Dependency in Bamboo Data Center and Server	All versions including and after 9.1.0	8.8	High
CVE-2023-5072	DoS org.json:json Dependency in Bamboo Data Center and Server	All versions including and after 9.2.3	7.5	High
CVE-2023-46589	Request Smuggling org.apache.tomcat:tomcat-catalina Dependency in Bamboo Data Center and Server	All versions including and after 9.2.1	7.5	High
CVE-2022-40152	DoS com.fasterxml.woodstox:woodstox-c	All versions including and	7.5	High

Flash | Disclosure of Critical Atlassian Confluence Vulnerability

F-2024-01-17a

TLP: CLEAR



CVE	Description	Affected Versions	CVSS v3.x ¹	Severity
	ore Dependency in Bamboo Data Center and Server	after 9.2.1		

Table 1. Vulnerabilities patched by Atlassian's security update on January 16, 2024

Source:

[hXXps://confluence.atlassian\[.\]com/security/security-bulletin-january-16-2024-1333335615.html](https://confluence.atlassian[.]com/security/security-bulletin-january-16-2024-1333335615.html)

| Appendix B: 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.

| Appendix C: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%