Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Security Vulnerabilities Discovered in Atlassian Products

Date of Publication	Admiralty Code	TA Number
September 26, 2023	A1	TA2023387

Summary

Discovered On: September 19, 2023
Affected Product: Jira Service Management Data Center and Server, Confluence Data Center and Server, Bitbucket Data Center and Server, Bamboo Data Center and Server
Impact: Atlassian have revealed the existence of several security vulnerabilities, namely CVE-2022-25647, CVE-2023-22512, CVE-2023-22513, and CVE-2023-28709, which affect their products. These vulnerabilities have the potential to be exploited, leading to denial-of-service (DoS) attacks and remote code execution.

CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2022-25647	Atlassian Jira Deserialization Flaw Vulnerability	Jira Service Management Server and Data Center	✗	✗	✓
CVE-2023-22512	Atlassian Confluence Denial of Service (DoS) Vulnerability	Confluence Data Center and Server	✗	✗	✓
CVE-2023-22513	Atlassian Bitbucket Remote Code Execution Vulnerability	Bitbucket Data Center and Server	✗	✗	✓
CVE-2023-28709	Atlassian Bamboo Denial of Service (DoS) Vulnerability	Bamboo Data Center and Server	✗	✗	✓

Vulnerability Details

#1 Atlassian have made public the existence of four high-severity vulnerabilities, namely CVE-2022-25647, CVE-2023-22512, CVE-2023-22513, and CVE-2023-28709, affecting its products. These vulnerabilities have the potential to be exploited, allowing attackers to achieve denial-of-service (DoS) attacks and remote code execution.

#2 CVE-2022-25647 is identified as a deserialization vulnerability affecting Patch Management within Jira Service Management Data Center and Server. This vulnerability stems from the deserialization of untrusted data via the internal classes' writeReplace() method. An attacker can send a carefully crafted request, which could potentially lead to a Denial-of-Service (DoS) situation.

#3 CVE-2023-22512 is categorized as a Denial-of-Service (DoS) vulnerability found in Confluence Data Center and Server. This vulnerability arises from the inadequate handling of internal resources within the application. A remote, non-authenticated attacker has the capability to send specifically crafted data to the application, enabling them to carry out a denial of service (DoS) attack.

#4 CVE-2023-22513 is identified as a Remote Code Execution (RCE) vulnerability occurring in Bitbucket Data Center and Server. This vulnerability allows an authenticated attacker to execute arbitrary code, and in some attack scenarios, it does not require any user interaction for exploitation.

#5 CVE-2023-28709 impacts Bamboo Data Center and Server editions and is linked to the incomplete resolution of CVE-2023-24998, a vulnerability that affected various versions of Apache Tomcat. In cases where non-default HTTP connector settings were applied, and the query string parameters reached the threshold specified by maxParameterCount, a request containing precisely maxParameterCount parameters in the query string could potentially circumvent the predefined limit for uploaded request parts. This vulnerability, if exploited, may result in a denial of service (DoS).

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-25647	Jira Service Management Server and Data Center (versions 4.20.0-4.20.24, 5.4.0-5.4.8, 5.9.0, 5.9.1, 5.10.0, 5.6.0, 5.7.0, 5.7.2, 5.8.1)	cpe:2.3:a:atlassian:jira_service_management_server_and_data_center:*:*:*:*:*:*:*:*	CWE-502
CVE-2023-22512	Confluence Server and Data Center (versions 5.6 and higher; except versions 7.19.14 and 8.5.1)	cpe:2.3:a:atlassian:confluence_server_and_data_center:8.5.0:*:*:*:*:*:*:*	CWE-399
CVE-2023-22513	Bitbucket Server and Data Center (versions 8.0-8.8, 8.9.0-8.9.4, 8.10.0-8.10.4, 8.11.0-8.11.3, 8.12.0-8.12.1, 8.13.0)	cpe:2.3:a:atlassian:bitbucket_data_center:*:*:*:*:*:*:*:*	CWE-20
CVE-2023-28709	Bamboo Server and Data Center (version 9.3.0, 9.2.0-9.2.3, 8.1, 8.2.)	cpe:2.3:a:atlassian:bamboo_server_and_data_center:*:*:*:*:*:*:*:*	CWE-193

Recommendations

Apply Patch: Install the security patch provided by Atlassian to address the CVE-2022-25647, CVE-2023-22512, CVE-2023-22513, and CVE-2023-28709 vulnerabilities. This patch closes the security gap that allows attackers to exploit the vulnerability.

Firewall and Access Control: Set up strong firewall rules and access policies to prevent unauthorized system access.

Security Hardening: Follow best practices for security hardening of your systems and applications to reduce the attack surface.

Network Segmentation: Segment your network into zones with different trust levels to restrict lateral movement of attackers

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0040 Impact	TA0001 Initial Access
TA0007 Discovery	T1588.005 Exploits	T1588 Obtain Capabilities	T1499 Endpoint Denial of Service
T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application		

Patch Details

Atlassian have release the new versions, upgrade to following versions to address the vulnerabilities:
Jira Service Management Server and Data Center version 4.20.25, 5.4.9, 5.9.2, 5.10.1, 5.11.0 or latest
Confluence Server and Data Center version 7.19.13, 7.19.14, 8.5.1, 8.6.0 or latest
Bitbucket Server and Data Center version 8.9.5, 8.10.5, 8.11.4, 8.12.2, 8.13.1, 8.14.0 or latest
Bamboo Server and Data Center version 9.2.4, 9.3.1 or latest

https://www.atlassian.com/software/jira/service-management/download-archives

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

https://www.atlassian.com/software/bitbucket/download-archives

https://www.atlassian.com/software/bamboo/download-archives

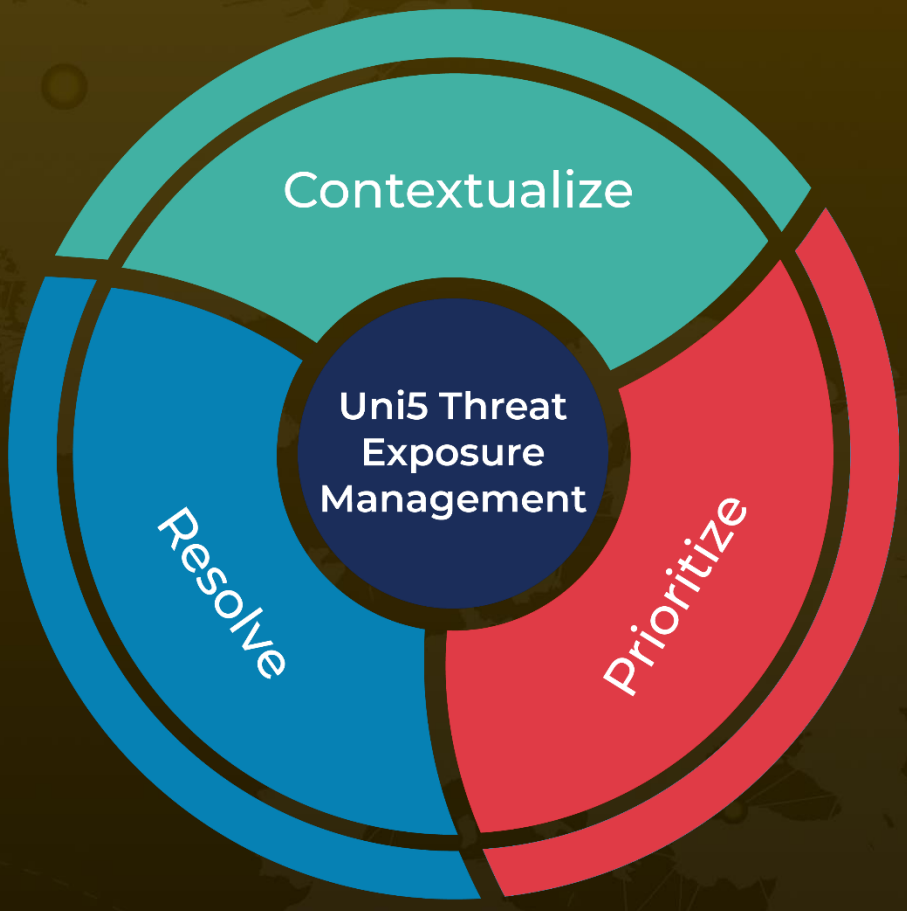
References

https://confluence.atlassian.com/security/security-bulletin-september-19-2023-1283691616.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

September 26, 2023 . 7:30 AM

More at www.hivepro.com