Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical SQL Injection Vulnerability Discovered in Atlassian Bamboo

Date of Publication	Admiralty Code	TA Number
March 22, 2024	A1	TA2024115

Summary

Discovered On: February 2024
Affected Products: Bamboo Data Center and Server
Impact: Atlassian has released patches addressing several security vulnerabilities, including a significant critical issue impacting Bamboo Data Center and Server, identified as CVE-2024-1597. This flaw, leading to a SQL injection, poses a risk of unnecessary data exposure and potential data manipulation.

⚙ CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-1597	Atlassian Bamboo Data Center and Server SQL injection Vulnerability	Bamboo Data Center and Server	✗	✓	✓

Vulnerability Details

#1 Atlassian addressed patches for numerous vulnerabilities throughout its product suite, including a critical-severity flaw, CVE-2024-1597, which is notable for its exploitation potential without user intervention. This vulnerability, stemming from PostgreSQL Maven package, poses a significant risk to various products including Atlassian Bamboo's server and data centers. Its capacity to enable SQL injection attacks underscores the urgent need for mitigation measures to safeguard affected systems from potential exploitation.

#2 The flaw arises from the usage of a minus sign (-) with a numeric literal, followed by a string on the same line. Additionally, it requires the simple query mode, which needs to be explicitly set using PreferQueryMode=SIMPLE, an option that is non-default. Attackers can exploit this by crafting a payload that matches the query structure to circumvent the protection of parameterized queries, thereby leading to SQL injection.

#3

This vulnerability is exploitable by unauthenticated attackers without requiring any user intervention, potentially leading to unauthorized access to read, write or modify the information. Atlassian also released security patches for Jira Software's Data Centre and Server, addressing a total of 20 high-severity vulnerabilities.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-1597	Bamboo Data Center and Server: Versions 9.5.0 to 9.5.1, 9.4.0 to 9.4.3, 9.3.0 to 9.3.6, 9.2.0 to 9.2.11 (LTS), 9.1.0 to 9.1.3, 9.0.0 to 9.0.4, 8.2.0 to 8.2.9, and earlier versions	cpe:2.3:a:postgresql:postgresql_jdbc_driver:*:*:*:*:*:*:*	CWE-89

Recommendations

Apply Patch: Install the security patch provided by Atlassian to address the CVE-2024-1597 vulnerability. This patch closes the security gap that allows attackers to exploit the vulnerability.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Deploy Behavioral Analysis Solutions: Utilize behavioral analysis solutions to detect any anomalous behavior on systems. Ensure that endpoint protection solutions are regularly updated to identify and mitigate the latest threats.

Utilize a DAM tool: DAM tools will monitor database activity in real-time and alert administrators to suspicious events or unauthorized access attempts. This proactive approach helps organizations detect and respond to security threats, including SQL injections, before they escalate into major incidents.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0004 Privilege Escalation	TA0040 Impact
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application	T1565 Data Manipulation

Patch Details

Atlassian has released patches to address the CVE-2024-1597 in the latest versions 9.6.0 (LTS), 9.5.2, 9.4.4, and 9.2.12 (LTS)

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

References

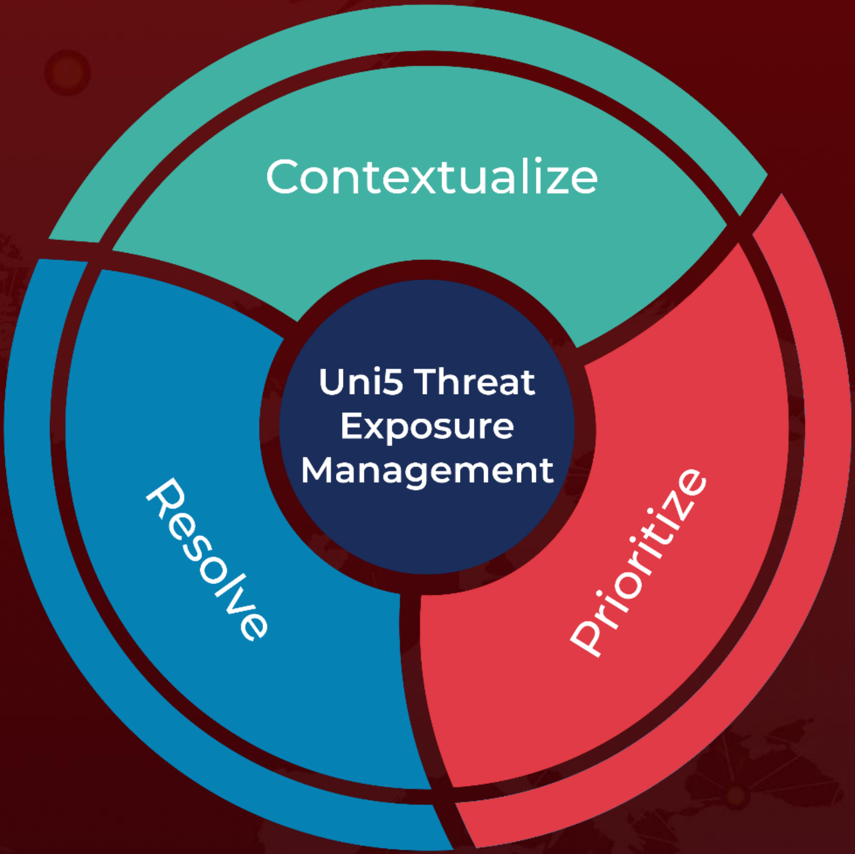
https://jira.atlassian.com/browse/BAM-25716

https://confluence.atlassian.com/security/security-bulletin-march-19-2024-1369444862.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

March 22, 2024 • 7:45 AM

More at www.hivepro.com