Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

An Authentication Vulnerability Discovered in Jira Service Management Server and Data Center

Date of Publication	Admiralty Code	TA Number
February 09, 2023	A1	TA2023072

Summary

First Seen: January 12, 2023
Affected Product: Jira Service Management Server and Data Center
Impact: The vulnerability allows an attacker to impersonate another user and gain access to a Jira Service Management instance under certain circumstances.

CVEs

CVE	NAME	PATCH
CVE-2023-22501	Broken Authentication vulnerability in Jira Service Management	✓

Vulnerability Details

A security vulnerability was found in Jira Service Management Server and Data Center (versions 5.3.0 to 5.5.0) which allows an attacker to access a Jira Service Management instance by impersonating another user. The vulnerability is present when the attacker has write access to a User Directory and outgoing email is enabled. The attacker could obtain access to signup tokens sent to users who have never logged into their account either by being included on Jira issues or requests with these users or by gaining access to emails containing a "View Request" link. Bot accounts and external customer accounts are particularly vulnerable.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-22501	Jira Service Management Server and Data Center (versions 5.3.0 to 5.5.0)	cpe:2.3:a:atlassian:jira_service_management:*:*:*:*:*:*:*:*	CWE-287

Recommendations

Security Leaders

Asset and vulnerability management solutions should be implemented to ensure that all internet-accessible devices are secure, patched, updated, hardened, and monitored. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize the vulnerability, identify the impacted assets, and patch them through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Patch Details' on the following pages.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation
TA0003 Persistence	TA0006 Credential Access	T1134.003 Make and Impersonate Token	T1556 Modify Authentication Process
T1134 Access Token Manipulation	T1078 Valid Accounts	T1588.006 Vulnerabilities	T1588 Obtain Capabilities

Patch Details

Upgrade to versions 5.3.3, 5.4.2, 5.5.1, 5.6.0 or later.

Links:
https://confluence.atlassian.com/jira/jira-service-management-server-and-data-center-advisory-cve-2023-22501-1188786458.html

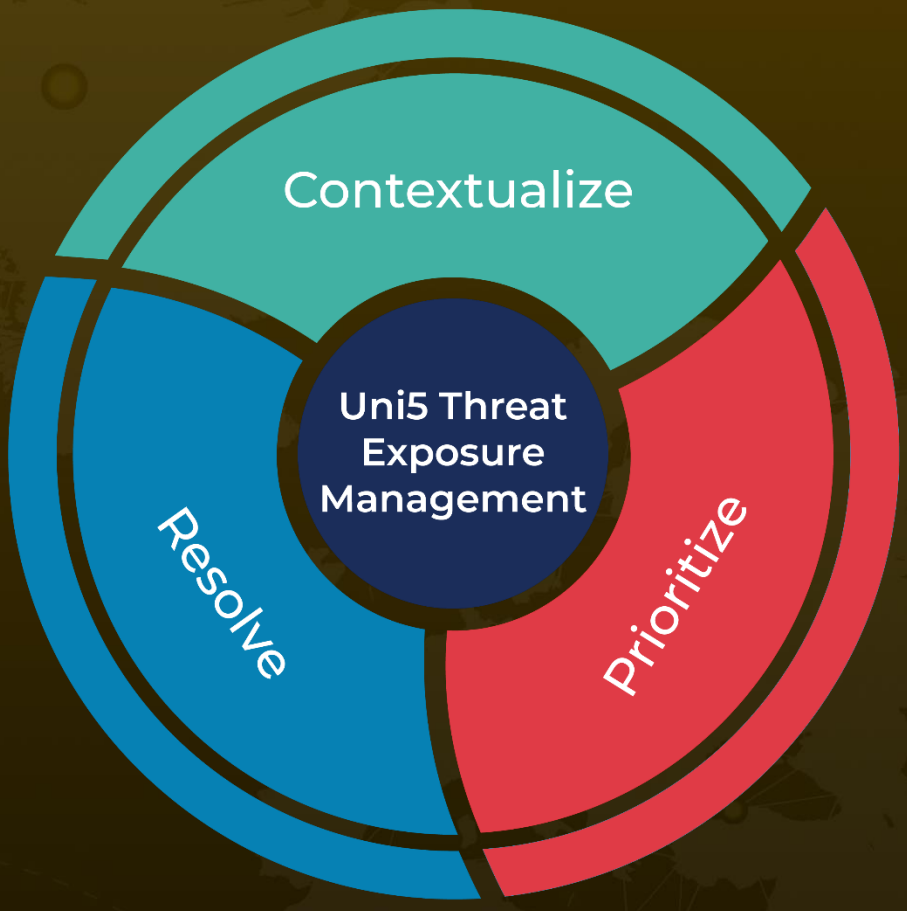
References

https://jira.atlassian.com/browse/JSDSERVER-12312

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

February 09, 2023 • 4:30 AM

More at www.hivepro.com