

THREAT ADVISORY

 **VULNERABILITY REPORT**

Atlassian Addresses Issues in Crowd and Bitbucket Products

Date of Publication

November 22, 2022

Admiralty Code

A1

TA Number

TA2022267



Summary

First Seen: November 16, 2022

Affected Products: Bitbucket Server, Crowd products, and Data Center.

Impact: Execute arbitrary code on the system

CVEs

CVE	NAME	PATCH
CVE-2022-43782	Critical security misconfiguration vulnerability	
CVE-2022-43781	Command Injection Vulnerability	

Vulnerability Details

Atlassian has two security holes that can be abused to allow arbitrary code execution. CVE-2022-43782 allows an intruder connecting from an IP address on the allow list to authenticate as the crowd application by evading the password validation. The attacker may then exploit the user-management path to access privileged endpoints in Crowd's REST API. The command injection vulnerability (CVE-2022-43781) in Bitbucket Server and Data Center is exploited by using environment variables in the software. An attacker with access to credentials can leverage this flaw to achieve code execution and execute code on the system.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-43782	Crowd: 3.0 - 5.0.2	cpe:2.3:a:atlassian: crowd:*:*:*:*:*:*: *	CWE-287
CVE-2022-43781	Bitbucket Server and Data Center: 7.0 - 7.21 and 8.0 - 8.4 (only if mesh.enabled is set to false in bitbucket.properties).	cpe:2.3:a:atlassian: bitbucket:*:*:*:*:*: *:*.*	CWE-77

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

<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0003</u> Persistence
<u>TA0008</u> Lateral Movement	<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities	<u>T1078</u> Valid Accounts
<u>T1098</u> Account Manipulation	<u>T1203</u> Exploitation for Client Execution	<u>T1190</u> Exploit Public-Facing Application	<u>T1574</u> Hijack Execution Flow
<u>T1210</u> Exploitation of Remote Services			

Patch Links

<https://jira.atlassian.com/browse/CWD-5888>

<https://jira.atlassian.com/browse/BSERV-13522>

References

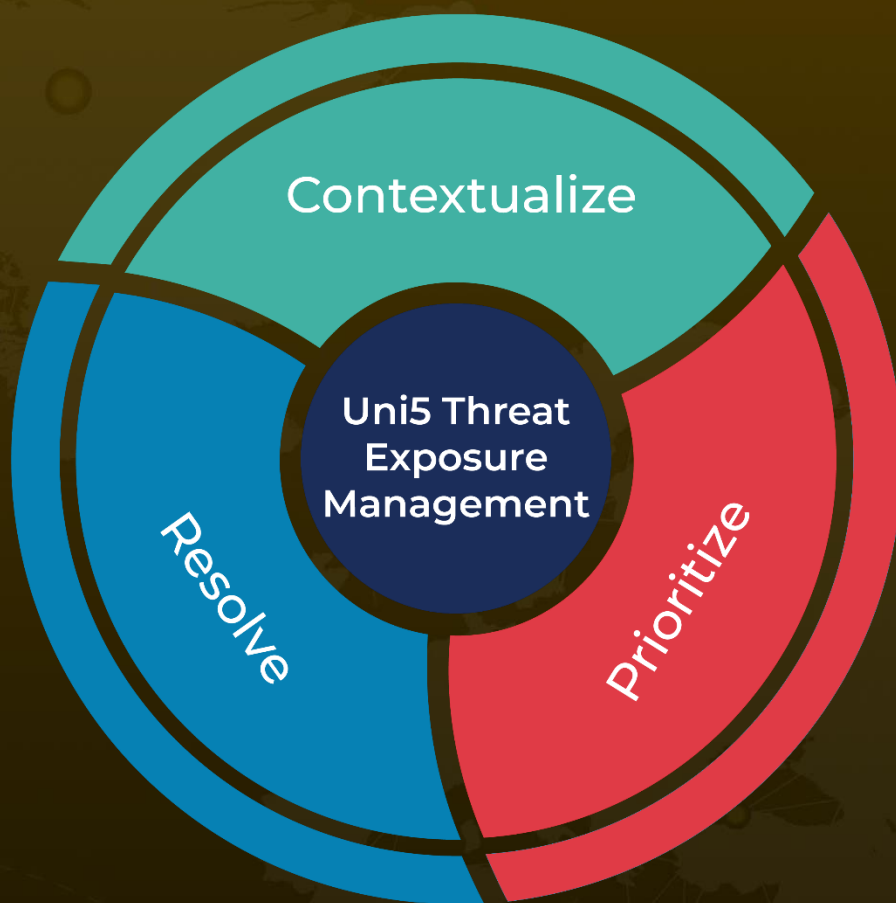
<https://confluence.atlassian.com/crowd/crowd-security-advisory-november-2022-1168866129.html>

<https://confluence.atlassian.com/bitbucketserver/bitbucket-server-and-data-center-security-advisory-2022-11-16-1180141667.html>

What Next?

At **HivePro**, 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 **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

November 22, 2022 • 3:33 AM

© 2022 All Rights are Reserved by HivePro



More at www.hivepro.com