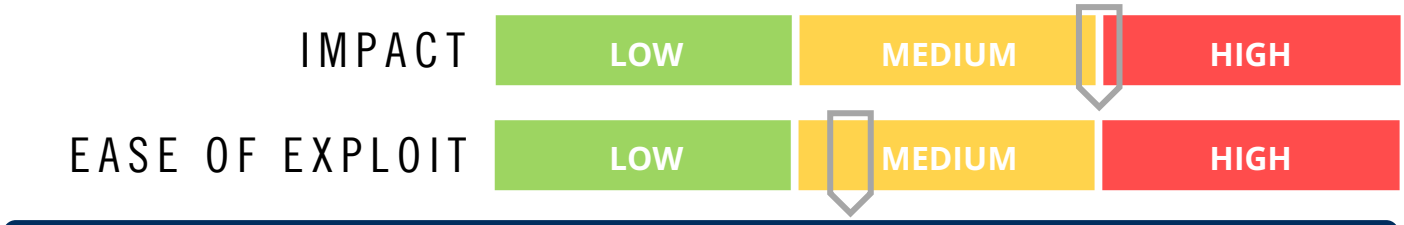
UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0263

ATLASSIAN RELEASES PATCHES FOR CRITICAL FLAWS

DATE ISSUED: 21st November 2022



OVERVIEW

Atlassian's security support advisory has released security updates for two critical vulnerabilities affecting Bitbucket Server, Data Center, and Crowd products.

BREAKDOWN

The first vulnerability, CVE-2022-43871, is introduced in version 7.0.0 of Bitbucket Server and Data Center which allows shell injection using environment variables in the software. An attacker with permissions enabled that allows the control of a username can exploit this vulnerability to gain code execution privileges and has the potential to then execute malicious code on the system. The second is a critical severity security misconfiguration vulnerability in the Crowd Server and Data Center - CVE-2022-43872, introduced in Crowd 3.0.0 versions. This allows attackers to authenticate themselves on the Crowd application by bypassing a password check. This could allow the attacker to call privileged endpoints in Crowd's REST API under the user-management path. This attack is only possible if the bad actor is connecting from an IP address that is added to the Remote Access configuration.

REMEDIATION STEPS

- Upgrade each affected product installation to a fixed version.
- Mitigate the issue by removing or validating any remote addresses for the crowd application in the Crowd product.
- Create strong passwords for all accounts on the computer.
- Be wary when granting access permission to applications in your cloud environment.

REFERENCES & RESOURCES

The Hacker News:	https://thehackernews.com/2022/11/atlassian-releases-patches-for-critical.html
Atlassian:	https://confluence.atlassian.com/bitbucketserver/bitbucket-server-and-data-center-security-advisory-2022-11-16-1180141667.html
Crowd Support	https://confluence.atlassian.com/crowd/crowd-5-0-release-notes-1127257883.html