

CVE-2022-36804

Atlassian Bitbucket Server and Data Center Command Injection Vulnerability

CISA KEV since Sep 30, 2022

Actively exploited

Public exploit module (Metasploit)

Multiple API endpoints in Atlassian Bitbucket Server and Data Center 7.0.0 before version 7.6.17, from version 7.7.0 before version 7.17.10, from version 7.18.0 before version 7.21.4, from version 8.0.0 before version 8.0.3, from version 8.1.0 before version 8.1.3, and from version 8.2.0 before version 8.2.2, and from version 8.3.0 before 8.3.1 allows remote attackers with read permissions to a public or private Bitbucket repository to execute arbitrary code by sending a malicious HTTP request. This vulnerability was reported via our Bug Bounty Program by TheGrandPew.

EVRS 86/100 Immediate priority	CVSS V3.1 8.8 High · NVD	EPSS 0.992 99.94th percentile · FIRST	CISA DEADLINE Oct 21, 2022 KEV since 2022 · listed over a year
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.992 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
bitbucket	≥ 7.0.0 < 7.6.17 ≥ 7.7.0 < 7.17.10 ≥ 7.18.0 < 7.21.4 ≥ 8.0.0 < 8.0.3 ≥ 8.1.0 < 8.1.3 ≥ 8.2.0 < 8.2.2 8.3.0	7.6.17 · 7.17.10 · 7.21.4 · 8.0.3 · 8.1.3 · 8.2.2	NVD

Sources

Vendor guidance	jira.atlassian.com/browse/BSERV-13438	NVD	nvd.nist.gov/vuln/detail/CVE-2022-36804
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2022-39504
Current data	evulnable.com/vulnerability-management/cve/CVE-2022-36804		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.