

CVE-2022-26138

Atlassian Questions For Confluence App Hard-coded Credentials Vulnerability

Exigent

CISA KEV since Jul 29, 2022

Actively exploited

The Atlassian Questions For Confluence app for Confluence Server and Data Center creates a Confluence user account in the confluence-users group with the username disabledsystemuser and a hardcoded password. A remote, unauthenticated attacker with knowledge of the hardcoded password could exploit this to log into Confluence and access all content accessible to users in the confluence-users group. This user account is created when installing versions 2.7.34, 2.7.35, and 3.0.2 of the app.

EVRS 87 / 100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.982 99.92nd percentile · FIRST	CISA DEADLINE Aug 19, 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	0.982 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent 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
questions for confluence	2.7.34 2.7.35 3.0.2	no fixed version listed	NVD
confluence data center	—	no fixed version listed	NVD
confluence server	—	no fixed version listed	NVD

Sources

Vendor guidance	jira.atlassian.com/browse/CONFSERVER-79483	Additional guidance	confluence.atlassian.com/doc/confluence-security-advisory-2022-07-20-1142446709.html nvd.nist.gov/vuln/detail/CVE-2022-26138
confluence.atlassian.com	confluence.atlassian.com/doc/questions-for-confluence-security-advisory-2022-07-20-1142446709.html	NVD	
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2022-30705
Current data	evulnable.com/vulnerability-management/cve/CVE-2022-26138		

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