Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-26134
State	PUBLIC
Assigner	security@atlassian.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-03 22:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	In affected versions of Confluence Server and Data Center, an OGNL injection vulnerability exists that would allow an unau

Risk And Classification

EPSS: 0.944080000 probability, percentile 0.999780000 (date 2026-05-12)

CISA KEV: Listed on 2022-06-02; due 2022-06-06; ransomware use Known

Problem Types: CWE-917

CISA Known Exploited Vulnerability

Vendor	Atlassian
Product	Confluence Server/Data Center
Name	Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability
Required Action	Immediately block all internet traffic to and from affected products AND apply the update per vendor instructions [https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html] OR remove the affected products by the due date on the right. Note: Once the update is successfully deployed, agencies can reassess the internet blocking rules.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2022-26134

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Confluence Data Center	All	All	All	All
Application	Atlassian	Confluence Data Center	7.18.0	All	All	All
Application	Atlassian	Confluence Server	All	All	All	All
Application	Atlassian	Confluence Server	7.18.0	All	All	All

References

Reference
Confluence Security Advisory 2022-06-02 | Confluence Data Center and Server 7.18 | Atlassian Documentation
Confluence OGNL Injection Remote Code Execution ≈ Packet Storm
Through The Wire CVE-2022-26134 Confluence Proof Of Concept ≈ Packet Storm
Confluence OGNL Injection Proof Of Concept ≈ Packet Storm
Atlassian Confluence Namespace OGNL Injection ≈ Packet Storm
[CONFSERVER-79016] Remote code execution via OGNL injection in Confluence Server & Data Center - CVE-2022-26134 - Create and trac
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

150523 Atlassian Confluence Server and Data Center OGNL Injection Remote Code Execution (RCE) Vulnerability (CVE-2022-26134)

376657 Atlassian Confluence Server and Confluence Data Center Remote Code Execution (RCE) Vulnerability (CONFSERVER-79016)

730514 Atlassian Confluence Server and Confluence Data Center Remote Code Execution (RCE) Vulnerability (CONFSERVER-79016) (Unauthenticated Check)

730515 Update TITLE manually (CONFSERVER-79016)