

# CVE-2021-26084

## Atlassian Confluence Server and Data Center Object-Graph Navigation Language (OGNL) Injection Vulnerability

Exigent
CISA KEV since Nov 3, 2021
Actively exploited
Ransomware use known
Public exploit module (Metasploit)

In affected versions of Confluence Server and Data Center, an OGNL injection vulnerability exists that would allow an unauthenticated attacker to execute arbitrary code on a Confluence Server or Data Center instance. The affected versions are before version 6.13.23, from version 6.14.0 before 7.4.11, from version 7.5.0 before 7.11.6, and from version 7.12.0 before 7.12.5.

|                                                            |                                                  |                                                           |                                                                                    |
|------------------------------------------------------------|--------------------------------------------------|-----------------------------------------------------------|------------------------------------------------------------------------------------|
| <b>EVRS</b><br><b>94</b> /100<br><b>Immediate</b> priority | <b>CVSS V3.1</b><br><b>9.8</b><br>Critical · NVD | <b>EPSS</b><br><b>0.999</b><br>99.99th percentile · FIRST | <b>CISA DEADLINE</b><br><b>Nov 17, 2021</b><br>KEV since 2021 · listed over a year |
|------------------------------------------------------------|--------------------------------------------------|-----------------------------------------------------------|------------------------------------------------------------------------------------|

### Signals behind the score

☒ counted in the score
 ☐ not counted
 evidence for 6 of 8 signals

|                                                       |                            |                                                                |                                            |
|-------------------------------------------------------|----------------------------|----------------------------------------------------------------|--------------------------------------------|
| <input checked="" type="checkbox"/> <b>CISA KEV</b>   | Listed in the catalog      | <input type="checkbox"/> <b>Vendor exploitation</b>            | Confirmed exploitation in the wild         |
| <input checked="" type="checkbox"/> <b>Ransomware</b> | Known ransomware campaigns | <input type="checkbox"/> <b>KEV recency</b>                    | On the CISA KEV catalog for over two years |
| <input checked="" type="checkbox"/> <b>EPSS</b>       | 0.999 probability          | <input type="checkbox"/> <b>Pre-patch disclosure</b>           | Disclosure status unavailable              |
| <input checked="" type="checkbox"/> <b>CVSS</b>       | Base score 9.8             | <input type="checkbox"/> <b>Microsoft Exploitability Index</b> | 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 |
|------------------------|-------------------------------------------------------------------------|------------------------------------|--------|
| confluence data center | < 6.13.23<br>≥ 6.14.0 < 7.4.11<br>≥ 7.5.0 < 7.11.6<br>≥ 7.12.0 < 7.12.5 | 6.13.23 · 7.4.11 · 7.11.6 · 7.12.5 | NVD    |
| confluence server      | < 6.13.23<br>≥ 6.14.0 < 7.4.11<br>≥ 7.5.0 < 7.11.6<br>≥ 7.12.0 < 7.12.5 | 6.13.23 · 7.4.11                   | NVD    |

### Sources

|                        |                                                                                                                                           |                   |                                                                                                                             |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>Vendor guidance</b> | <a href="https://jira.atlassian.com/browse/CONFSERVER-67940">jira.atlassian.com/browse/CONFSERVER-67940</a>                               | <b>NVD</b>        | <a href="https://nvd.nist.gov/vuln/detail/CVE-2021-26084">nvd.nist.gov/vuln/detail/CVE-2021-26084</a>                       |
| <b>CISA KEV</b>        | <a href="https://cisa.gov/known-exploited-vulnerabilities-catalog">cisa.gov/known-exploited-vulnerabilities-catalog</a>                   | <b>ENISA EUVD</b> | <a href="https://euvd.enisa.europa.eu/vulnerability/EUVD-2021-12905">euvd.enisa.europa.eu/vulnerability/EUVD-2021-12905</a> |
| <b>Current data</b>    | <a href="https://evulnable.com/vulnerability-management/cve/CVE-2021-26084">evulnable.com/vulnerability-management/cve/CVE-2021-26084</a> |                   |                                                                                                                             |

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