

# CVE-2019-11581

## Atlassian Jira Server and Data Center Server-Side Template Injection Vulnerability

CISA KEV since Mar 7, 2022

Actively exploited

There was a server-side template injection vulnerability in Jira Server and Data Center, in the ContactAdministrators and the SendBulkMail actions. An attacker is able to remotely execute code on systems that run a vulnerable version of Jira Server or Data Center. All versions of Jira Server and Data Center from 4.4.0 before 7.6.14, from 7.7.0 before 7.13.5, from 8.0.0 before 8.0.3, from 8.1.0 before 8.1.2, and from 8.2.0 before 8.2.3 are affected by this vulnerability.

|                                                                |                                                          |                                                                   |                                                                                           |
|----------------------------------------------------------------|----------------------------------------------------------|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| <p>EVRS</p> <p><b>83</b>/100</p> <p><b>Urgent</b> priority</p> | <p>CVSS V3.1</p> <p><b>9.8</b></p> <p>Critical · NVD</p> | <p>EPSS</p> <p><b>0.846</b></p> <p>99.71st percentile · FIRST</p> | <p>CISA DEADLINE</p> <p><b>Sep 7, 2022</b></p> <p>KEV since 2022 · listed over a year</p> |
|----------------------------------------------------------------|----------------------------------------------------------|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------|

### 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 type="checkbox"/> <b>Ransomware</b>          | No known ransomware campaign association | <input type="checkbox"/> <b>KEV recency</b>                    | On the CISA KEV catalog for over two years |
| <input checked="" type="checkbox"/> <b>EPSS</b>     | 0.846 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

**Patch This Cycle** 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 |
|-------------|----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|--------|
| jira server | $\geq 4.4 < 7.6.14$<br>$\geq 7.7.0 < 7.13.5$<br>$\geq 8.0.0 < 8.0.3$<br>$\geq 8.1.0 < 8.1.2$<br>$\geq 8.2.0 < 8.2.3$ | $7.6.14 \cdot 7.13.5 \cdot 8.0.3 \cdot$<br>$8.1.2 \cdot 8.2.3$ | NVD    |

### Sources

**Vendor guidance** [github.com/advisories/GHSA-55hv-x43w-phcv](https://github.com/advisories/GHSA-55hv-x43w-phcv)  
**NVD** [nvd.nist.gov/vuln/detail/CVE-2019-11581](https://nvd.nist.gov/vuln/detail/CVE-2019-11581)

**Additional guidance** [jira.atlassian.com/browse/JRASERVER-69532](https://jira.atlassian.com/browse/JRASERVER-69532)  
**CISA KEV** [cisa.gov/known-exploited-vulnerabilities-catalog](https://cisa.gov/known-exploited-vulnerabilities-catalog)

**ENISA EUVD** [euvd.enisa.europa.eu/vulnerability/EUVD-2019-3251](https://euvd.enisa.europa.eu/vulnerability/EUVD-2019-3251)

**Current data** [evulnable.com/vulnerability-management/cve/CVE-2019-11581](https://evulnable.com/vulnerability-management/cve/CVE-2019-11581)

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