

# Security Bulletin - April 21 2026

## April 2026 Security Bulletin

The vulnerabilities reported in this Security Bulletin include 31 high-severity vulnerabilities and 7 critical-severity third-party vulnerabilities, which have been fixed in new versions of our products released in the last month.

CVEs reported in monthly Security Bulletins have been assessed as presenting a non-critical risk to Atlassian customers. Atlassian issues Critical Security Advisories for vulnerabilities that pose an immediate critical risk based on how our products actually use the affected components outside of our monthly Security Bulletin schedule as necessary.

Vulnerabilities are discovered through our Bug Bounty program, pen-testing processes, and third-party library scans.

## INSTRUCTIONS

To fix all the vulnerabilities impacting your product(s), Atlassian recommends patching your instances to the latest version or one of the Fixed Versions for each product below. The listed Fixed Versions for each product are current as of April 21, 2026 (date of publication); visit the linked product Release Notes for the most up-to-date versions.

To search for CVEs or check your product versions for disclosed vulnerabilities, check the [Vulnerability Disclosure Portal](#).

Released Security Vulnerabilities						
Product & Release Notes	Affected Versions	Fixed Version	Vulnerability Summary	CVE ID	CVSS Severity	
<a href="#">Bamboo Data Center and Server</a>	<ul style="list-style-type: none"> <li>12.1.0 to 12.1.3 (LTS)</li> <li>12.0.0 to 12.0.2</li> <li>11.0.0 to 11.0.8</li> <li>10.2.0 to 10.2.16 (LTS)</li> <li>10.1.0 to 10.1.1</li> <li>10.0.0 to</li> </ul>	<ul style="list-style-type: none"> <li>12.1.6 (LTS) recommended <b>Data Center Only</b></li> <li>10.2.18 (LTS) <b>Data Center Only</b></li> </ul>	<a href="#">DoS (Denial of Service) io.netty:netty-codec-http2 Dependency in Bamboo Data Center</a>	<a href="#">CVE-2026-33871</a>	8.7 High	
			<a href="#">OS Command Injection in Bamboo Data Center - CVE-2026-21571</a>	<a href="#">CVE-2026-21571</a>	9.4 Critical <i>This is a vulnerability in a non-Atlassian dependency. Atlassian's application of this dependency presents a lower, non-critical assessed risk.</i>	

	<ul style="list-style-type: none"> <li>10.0.3</li> <li>• 9.6.2 to 9.6.24 (LTS)</li> </ul>		<a href="#">HTTP Request Smuggling org.apache.tomcat:tomcat-catalina Dependency in Bamboo Data Center</a>	<a href="#">CVE-2026-24880</a>	7.5 High
			<a href="#">HTTP Request Smuggling io.netty:netty-codec-http Dependency in Bamboo Data Center</a>	<a href="#">CVE-2026-33870</a>	7.5 High
			<a href="#">MITM (Man-in-the-Middle) org.apache.tomcat:tomcat-coyote Dependency in Bamboo Data Center</a>	<a href="#">CVE-2026-24734</a>	7.5 High
			<a href="#">DoS (Denial of Service) axios Dependency in Bamboo Data Center</a>	<a href="#">CVE-2026-25639</a>	7.5 High
			<a href="#">XSS (Cross Site Scripting) dompurify Dependency in Bamboo Data Center</a>	<a href="#">CVE-2024-45801</a>	7.3 High
<a href="#">Bitbucket Data Center and Server</a>	<ul style="list-style-type: none"> <li>• 10.1.1 to 10.1.5</li> <li>• 10.0.1 to 10.0.2</li> <li>• 9.4.12 to 9.4.17 (LTS)</li> </ul>	<ul style="list-style-type: none"> <li>• 10.2.0 to 10.2.2 (LTS) recommended <b>Data Center Only</b></li> <li>• 9.4.18 to 9.4.19 (LTS) <b>Data Center Only</b></li> </ul>	<a href="#">DoS (Denial of Service) ua-parser-js Dependency in Bitbucket Data Center</a>	<a href="#">CVE-2022-25927</a>	7.5 High
<a href="#">Confluence Data Center and Server</a>	<ul style="list-style-type: none"> <li>• 10.2.0 to 10.2.7 (LTS)</li> <li>• 10.1.0 to 10.1.2</li> <li>• 10.0.2 to 10.0.3</li> <li>• 9.5.1 to 9.5.4</li> </ul>	<ul style="list-style-type: none"> <li>• 10.2.10 (LTS) recommended <b>Data Center Only</b></li> <li>• 9.2.19 (LTS) <b>Data Center Only</b></li> </ul>	<a href="#">RCE (Remote Code Execution) org.yaml:snakeyaml Dependency in Confluence Data Center</a>	<a href="#">CVE-2022-1471</a>	9.8 Critical  <i>This is a vulnerability in a non-Atlassian Confluence dependency. Atlassian's application of this dependency presents a lower, non-</i>

- 9.4.0 to 9.4.1
- 9.3.1 to 9.3.2
- 9.2.0 to 9.2.17 (LTS)
- 9.1.0 to 9.1.1
- 9.0.1 to 9.0.3
- 8.9.1 to 8.9.8

			<i>critical assessed risk.</i>
	<a href="#">Path Traversal (Arbitrary Write) node-tar Dependency in Confluence Data Center</a>	<a href="#">CVE-2026-23950</a>	8.8 High
	<a href="#">DoS (Denial of Service) io.netty:netty-codec-http2 Dependency in Confluence Data Center</a>	<a href="#">CVE-2026-33871</a>	8.7 High
	<a href="#">Injection immutable Dependency in Confluence Data Center</a>	<a href="#">CVE-2026-29063</a>	8.7 High
	<a href="#">File Inclusion node-tar Dependency in Confluence Data Center</a>	<a href="#">CVE-2026-23745</a>	8.2 High
	<a href="#">File Inclusion node-tar Dependency in Confluence Data Center</a>	<a href="#">CVE-2026-24842</a>	8.2 High
	<a href="#">File Inclusion node-tar Dependency in Confluence Data Center</a>	<a href="#">CVE-2026-31802</a>	8.2 High
	<a href="#">DOM-based XSS @remix-run/router Dependency in Confluence Data Center</a>	<a href="#">CVE-2026-22029</a>	8 High
	<a href="#">DoS (Denial of Service) valibot Dependency in Confluence Data Center</a>	<a href="#">CVE-2025-66020</a>	7.5 High
	<a href="#">DoS (Denial of Service) org.bitbucket.b_c:jose4j Dependency in Confluence Data Center</a>	<a href="#">CVE-2024-29371</a>	7.5 High
	<a href="#">HTTP Request Smuggling io.netty:netty-codec-http Dependency in Confluence Data Center</a>	<a href="#">CVE-2026-33870</a>	7.5 High
	<a href="#">DoS (Denial of Service) axios Dependency in Confluence</a>	<a href="#">CVE-2026-</a>	7.5 High

			<a href="#">Data Center</a>	<a href="#">25639</a>		
			<a href="#">DoS (Denial of Service) css Dependency in Confluence Data Center</a>	<a href="#">CVE-2023-48631</a>	7.5 High	
			<a href="#">Injection dompurify Dependency in Confluence Data Center</a>	<a href="#">CVE-2024-45801</a>	7.3 High	
			<a href="#">File Inclusion node-tar Dependency in Confluence Data Center</a>	<a href="#">CVE-2026-26960</a>	7.1 High	
<a href="#">Jira Data Center and Server</a>	<ul style="list-style-type: none"> <li>• 11.3.0 to 11.3.3 (LTS)</li> <li>• 10.7.1 to 10.7.4</li> <li>• 10.6.0 to 10.6.1</li> <li>• 10.5.0 to 10.5.1</li> <li>• 10.4.0 to 10.4.1</li> <li>• 10.3.0 to 10.3.18 (LTS)</li> <li>• 10.2.0 to 10.2.1</li> <li>• 10.1.1 to 10.1.2</li> <li>• 10.0.0 to 10.0.1</li> <li>• 9.17.0 to 9.17.5</li> </ul>	<ul style="list-style-type: none"> <li>• 11.3.4 (LTS) recommended <b>Data Center Only</b></li> <li>• 10.3.19 (LTS) <b>Data Center Only</b></li> </ul>	<a href="#">mXSS (mutation Cross-Site Scripting) dompurify Dependency in Jira Software Data Center and Server</a>	<a href="#">CVE-2024-47875</a>	10 Critical	<i>This is a vulnerability in a non-Atlassian Jira Data Center dependency. Atlassian's application of this dependency presents a lower, non-critical assessed risk.</i>
			<a href="#">RCE (Remote Code Execution) org.yaml:snakeyaml Dependency in Jira Software Data Center</a>	<a href="#">CVE-2022-1471</a>	9.8 Critical	<i>This is a vulnerability in a non-Atlassian Jira Data Center dependency. Atlassian's application of this dependency presents a lower, non-critical assessed risk.</i>

	<ul style="list-style-type: none"> <li>• 9.16.0 to 9.16.1</li> <li>• 9.15.2</li> <li>• 9.12.8 to 9.12.33 (LTS)</li> </ul>		<p><a href="#">DoS (Denial of Service) brace-expansion Dependency in Jira Software Data Center</a></p>	<p><a href="#">CVE-2026-25547</a></p>	<p>9.2 Critical</p> <p><i>This is a vulnerability in a non-Atlassian Jira Data Center dependency. Atlassian's application of this dependency presents a lower, non-critical assessed risk.</i></p>
			<p><a href="#">Improper Authorization commons-beanutils:commons-beanutils Dependency in Jira Software Data Center</a></p>	<p><a href="#">CVE-2025-48734</a></p>	<p>8.8 High</p>
			<p><a href="#">MITM (Man-in-the-Middle) com.squareup.okhttp3:okhttp Dependency in Jira Software Data Center and Server</a></p>	<p><a href="#">CVE-2021-0341</a></p>	<p>7.5 High</p>
			<p><a href="#">DoS (Denial of Service) net.minidev:json-smart Dependency in Jira Software Data Center</a></p>	<p><a href="#">CVE-2023-1370</a></p>	<p>7.5 High</p>
			<p><a href="#">DoS (Denial of Service) com.squareup.okio:okio Dependency in Jira Software Data Center</a></p>	<p><a href="#">CVE-2023-3635</a></p>	<p>7.5 High</p>
<p><a href="#">Jira Service Management Data Center and Server</a></p>	<ul style="list-style-type: none"> <li>• 11.3.0 to 11.3.3 (LTS)</li> <li>• 11.2.0 to 11.2.1</li> <li>• 11.1.0 to 11.1.1</li> </ul>	<ul style="list-style-type: none"> <li>• 11.3.4 (LTS) recommended <b>Data Center Only</b></li> <li>• 10.3.19 (LTS) <b>Data Center Only</b></li> </ul>	<p><a href="#">mXSS (mutation Cross-Site Scripting) dompurify Dependency in Jira Service Management Data Center and Server</a></p>	<p><a href="#">CVE-2024-47875</a></p>	<p>10 Critical</p> <p><i>This is a vulnerability in a non-Atlassian Jira Service Management dependency. Atlassian's application of this</i></p>

- 11.0.1
- 10.7.1 to 10.7.4
- 10.6.0 to 10.6.1
- 10.5.0 to 10.5.1
- 10.4.0 to 10.4.1
- 10.3.0 to 10.3.18 (LTS)
- 10.2.0 to 10.2.1
- 10.1.1 to 10.1.2
- 10.0.0 to 10.0.1
- 5.17.0 to 5.17.5
- 5.16.0 to 5.16.1
- 5.15.2

			<i>dependency presents a lower, non-critical assessed risk.</i>
	<a href="#">RCE (Remote Code Execution) org.yaml:snakeyaml Dependency in Jira Service Management Data Center</a>	<a href="#">CVE-2022-1471</a>	9.8 Critical <i>This is a vulnerability in a non-Atlassian Jira Service Management dependency. Atlassian's application of this dependency presents a lower, non-critical assessed risk.</i>
	<a href="#">MITM (Man-in-the-Middle) xmlhttprequest Dependency in Jira Service Management Data Center</a>	<a href="#">CVE-2021-31597</a>	9.4 Critical <i>This is a vulnerability in a non-Atlassian Jira Service Management dependency. Atlassian's application of this dependency presents a lower, non-critical assessed risk.</i>
	<a href="#">Improper Authorization commons-beanutils:commons-beanutils Dependency in Jira Service Management Data Center</a>	<a href="#">CVE-2025-48734</a>	8.8 High
	<a href="#">DoS (Denial of Service) com.squareup.okio:okio</a>	<a href="#">CVE-2023-3635</a>	7.5 High

			Dependency in Jira Service Management Data Center		
			MITM (Man-in-the-Middle) com.squareup.okhttp3:okhttp Dependency in Jira Service Management Data Center and Server	CVE-2021-0341	7.5 High
			DoS (Denial of Service) brace-expansion Dependency in Jira Service Management Data Center	CVE-2026-25547	7.5 High
			DoS (Denial of Service) net.minidev:json-smart Dependency in Jira Service Management Data Center	CVE-2023-1370	7.5 High

## Frequently Asked Questions:

- **Why is my Feature Version not listed in a Fixed Version?** You may be using an unsupported version and need to patch to the latest version or Long-Term Support (LTS) version.
- **What are the most up-to-date Data Center product versions?** You can always check the [software download portal](#) or visit the product-specific download pages.
  - [Jira Software Data Center](#)
  - [Jira Service Management](#)
  - [Confluence Data Center](#)
  - [Bitbucket Data Center](#)
  - [Bamboo Data Center](#)
  - [Crowd Data Center](#)
- **I am using an LTS, why is it not listed in the Fixed Versions?** Your LTS version may not have been updated yet or a backported fix may not have been feasible. Please see our [Security Bug Fix Policy](#) for more information. We recommend upgrading your products to the latest versions. For the latest fixed versions, visit the release notes linked in the vulnerability table.
- **Questions about the bulletin, have feedback?** Let us know! Read more about our bulletins and feel free to contribute feedback on our latest [Community Post](#)

To search for CVEs or check your products versions for disclosed vulnerabilities, check the [Vulnerability Disclosure Portal](#).

