Confluence Security Advisory - 2021-08-25

Confluence Server and Data Center - CVE-2021-26084 - Confluence Server Webwork OGNL injection

Update: This advisory has been updated since its original publication.

Specific updates include:

- The vulnerability is being actively exploited in the wild.
  Affected servers should be patched immediately.
- The vulnerability is exploitable by unauthenticated users regardless of configuration.
- Minor text changes to clarify how customers can identify if they are using Confluence Cloud

If you have already upgraded to a fixed version, there is no further action required.

Summary	CVE-2021-26084 - Confluence Server Webwork OGNL injection
Advisory Release Date	25th August 2021 10AM PDT (Pacific Time, -7 hours)
Product	• Confluence Server • Confluence Data Center **Confluence Cloud customers are not affected.**
Affected versions	• All 4.x.x versions • All 5.x.x versions • All 6.0.x versions • All 6.1.x versions • All 6.2.x versions • All 6.3.x versions • All 6.4.x versions • All 6.5.x versions • All 6.6.x versions • All 6.7.x versions • All 6.8.x versions • All 6.9.x versions • All 6.10.x versions • All 6.11.x versions • All 6.12.x versions • All 6.13.x versions **before** 6.13.23 • All 6.14.x versions • All 6.15.x versions • All 7.0.x versions

Confluence Security Advisory 2006-01-23

Confluence 9.1 (Latest) Documentation

- Get started
- Spaces
- Pages and blogs
- Files
- Confluence Mobile
- Macros
- Your profile and settings
- Collaboration
- Analytics
- Search
- Permissions and restrictions
- Team Calendars
- Add-ons and integrations
- Confluence use-cases
- **Confluence administrator's guide**
  - Getting Started as Confluence Administrator
  - Manage Users
  - Managing System and Marketplace Apps
  - Writing User Macros
  - Customizing your Confluence Site
  - Integrating Confluence with Other Applications
  - Managing your Confluence License
  - Managing Confluence Data
  - Configuring Confluence
  - **Configuring Confluence Security**
    - **Confluence Security Overview and Advisories**
      - Confluence Community Security Advisory 2006-01-19

	• All 7.9.x versions • All 7.10.x versions • All 7.11.x versions **before** 7.11.6 • All 7.12.x versions **before** 7.12.5
Fixed versions	• 6.13.23 • 7.4.11 • 7.11.6 • 7.12.5 • 7.13.0
CVE ID(s)	CVE-2021-26084

Summary of Vulnerability

This advisory discloses a critical severity security vulnerability. Confluence Server and Data Center versions **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** are affected by this vulnerability.

Confluence Cloud sites are not affected.

If your Confluence site is accessed via an `atlassian.net` domain, it is hosted by Atlassian and you are not affected by the vulnerability.

Customers who have upgraded to versions 6.13.23, 7.11.6, 7.12.5, 7.13.0, or 7.4.11 are not affected.

Customers who have downloaded and installed any versions listed in the Affected Versions section must upgrade their installations to fix this vulnerability. If you are unable to upgrade immediately, apply the workaround detailed below while you plan your upgrade.

CVE-2021-26084 - Confluence Server Webwork OGNL injection

Severity

This vulnerability is being actively exploited in the wild.
Affected servers should be patched immediately.

Atlassian rates the severity level of this vulnerability as critical, according to the scale published in our Atlassian severity levels. The scale allows us to rank the severity as critical, high, moderate or low.

This is our assessment and you should evaluate its applicability to your own IT environment.

Description

An OGNL injection vulnerability exists that would allow an unauthenticated user to execute arbitrary code on a Confluence Server or Data Center instance.

All versions of Confluence Server and Data Center prior to the fixed versions listed above are affected by this vulnerability.

This issue can be tracked here:

Confluence Security Advisory 2006-01-23

Confluence 9.1 (Latest) Documentation

- Get started
- Spaces
- Pages and blogs
- Files
- Confluence Mobile
- Macros
- Your profile and settings
- Collaboration
- Analytics
- Search
- Permissions and restrictions
- Team Calendars
- Add-ons and integrations
- Confluence use-cases
- **Confluence administrator's guide**
  - Getting Started as Confluence Administrator
  - Manage Users
  - Managing System and Marketplace Apps
  - Writing User Macros
  - Customizing your Confluence Site
  - Integrating Confluence with Other Applications
  - Managing your Confluence License
  - Managing Confluence Data
  - Configuring Confluence
  - **Configuring Confluence Security**
    - **Confluence Security Overview and Advisories**
      - Confluence Community Security Advisory 2006-01-19

We have taken the following steps to address this issue:

- Released versions 6.13.23, 7.4.11, 7.11.6, 7.12.5, and 7.13.0 which contain a fix for this issue.

What You Need to Do

Atlassian recommends that you upgrade to the latest Long Term Support release. For a full description of the latest version, see the Confluence Server and Data Center Release Notes. You can download the latest version from the download centre.

If you are running an affected version **upgrade to version 7.13.0 (LTS) or higher**.

If you are running **6.13.x versions** and **cannot upgrade to 7.13.0 (LTS) then upgrade to version 6.13.23**.

If you are running **7.4.x versions** and **cannot upgrade to 7.13.0 (LTS) then upgrade to version 7.4.11**.

If you are running **7.11.x versions** and **cannot upgrade to 7.13.0 (LTS) then upgrade to version 7.11.6.**

If you are running **7.12.x versions** and **cannot upgrade to 7.13.0 (LTS) then upgrade to version 7.12.5**.

Mitigation

If you are unable to upgrade Confluence immediately, then as a **temporary** workaround, you can mitigate the issue by running the script below for the Operating System that Confluence is hosted on.

- Confluence Server or Data Center Node running on Linux based Operating System...
- Confluence Server or Data Center Node running on Microsoft Windows...

Support

If you did not receive an email for this advisory and you wish to receive such emails in the future go to https://my.atlassian.com/email and subscribe to Alerts emails.

If you have questions or concerns regarding this advisory, please raise a support request at https://support.atlassian.com/.

References

Security Bug fix Policy	As per our policy, critical security bug fixes will be back ported in accordance with https://www.atlassian.com/trust/security/bug-fix-policy. We will release new maintenance releases for the versions covered by the policy instead of binary patches. **Binary patches are no longer released.**
Severity Levels for security issues	Atlassian security advisories include a severity level and a CVE identifier. This severity level is based on our self-calculated CVSS score for each specific vulnerability. CVSS is an industry standard vulnerability metric. You can also learn more about CVSS at FIRST.org.
End of Life Policy	Our end of life policy varies for different products. Please refer to our EOL Policy for details.

Last modified on Sep 7, 2021