



Atlassian Confluence OGNL RCE Vulnerability

A critical vulnerability on Atlassian Confluence

<https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html>
 CVEs: [CVE-2022-26134](#)

A critical 0-day vulnerability on Atlassian Confluence Data Center and Server is actively being exploited in the wild. The vulnerability is established via the Object Graph Navigation Language (OGNL) injection that allows an unauthenticated user to execute arbitrary code.

Background A cybersecurity firm Volexity was responding to an attack incident, which revealed that the attack leveraged a 0-day vulnerability on Atlassian Confluence Server.

Announced June 2, 2022: The vendor has released an advisory.

Latest Developments June 2, 2022: The Hacker News posted an article on Volexity's discovery of the 0-day.
 June 3, 2022: The vendor has released their fixed.

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

- Reconnaissance
- Weaponization
- Delivery

Vulnerability

Blocks attack attempts related to Confluence OGNL vulnerability (CVE-2022-26134).

FortiClient
DB 1.315

Exploitation

IPS

Blocks attack attempts related to Confluence OGNL vulnerability (CVE-2022-26134).

FortiGate DB 21.331 FortiSASE DB 21.331 FortiNDR DB 21.331 FortiADC DB 21.331 FortiProxy DB 21.331

Installation

Post-execution

FortiEDR
v5.0+

C2

Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Threat Hunting

FortiEDR FortiSIEM v6.4+

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

Incident Response

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

NSE Training Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download and other forms of cyberattacks.

Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

Security Rating

Vulnerability Management

Reduce the attack surface on software vulnerabilities via systematic and automated patching.

FortiEDR

Additional Resources

CISA	https://www.cisa.gov/uscert/ncas/current-activity/2022/06/02/atlassian-releases-security-updates-confluence-server-and-data
Volexity	https://www.volexity.com/blog/2022/06/02/zero-day-exploitation-of-atlassian-confluence/
Hacker News	https://thehackernews.com/2022/06/hackers-exploiting-unpatched-critical.html
Threat Signal	https://www.fortiguard.com/threat-signal-report/4613

Learn more about [FortiGuard Outbreak Alerts](#)