OUTBREAK ALERTS

Confluence OGNL

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.

Cyber Kill Chain

Reconnaissance

Weaponization

Delivery

FortiClient
Vulnerability 1.315
Blocks attack attempts related to Confluence OGNL vulnerability (CVE-2022-26134).

Exploitation

FortiGate
IPS 21.331
Blocks attack attempts related to Confluence OGNL vulnerability (CVE-2022-26134).

FortiWeb
Web App Security 0.00251
Blocks attack attempts related to Confluence OGNL vulnerability (CVE-2013-2134/CVE-2022-26134).

FortiClient
Application Firewall 21.333
Blocks attack attempts related to Confluence OGNL vulnerability (CVE-2022-26134).

FortiSASE
IPS 21.331
Blocks attack attempts related to Confluence OGNL vulnerability (CVE-2022-26134).

FortiNDR
IPS 21.331
Blocks attack attempts related to Confluence OGNL vulnerability (CVE-2022-26134).

FortiADC
IPS 21.331
Blocks attack attempts related to Confluence OGNL vulnerability (CVE-2022-26134).

FortiProxy
IPS 21.331
Blocks attack attempts related to Confluence OGNL vulnerability (CVE-2022-26134).

Installation

FortiEDR
Post-Execution 4.0+
Detects post-exploitation behavior associated with the CVE-2022-26134 vulnerability.

C2

Action

Endpoint

Incident Response (Security Operations)

To help customers identify and protect vulnerable, FortiAnalyzer, FortiSIEM and FortiSOAR updates are available to raise alerts and escalate to incident response:

FortiAnalyzer	***Outbreak Detection*** Version 1.057 https://www.fortiguard.com/updates/outbreak-detection-service?version=1.00057 ***Threat Hunting*** Version 7.0+ https://community.fortinet.com/t5/FortiAnalyzer/Technical-Tip-Using-FortiAnalyzer-to-detect-Confluence-RCE-CVE/ta-p/213812
FortiSIEM	***Threat Hunting*** Version 6.4 https://help.fortinet.com/fsiem/6-4-0/Online-Help/HTML5_Help/content_updates.htm#Content9

Additional Resources

CISA Gov	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/
The Hacker News	https://thehackernews.com/2022/06/hackers-exploiting-unpatched-critical.html
Bleeping Computer	https://www.bleepingcomputer.com/news/security/critical-atlassian-confluence-zero-day-actively-used-in-attacks/
Threat Signal	https://www.fortiguard.com/threat-signal-report/4613