F#RTINET.

OUTBREAK ALERTS

A critical vulnverability 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.

Atlassian Confluence OGNL RCE Vulnerability

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

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

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

June 3, 2022: The vendor has released their fixed.



Announced

PROTECT

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

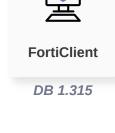
Weaponization

Reconnaissance

Delivery

Vulnerability

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



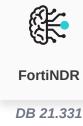
Exploitation

IPS

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











Installation

DB 21.331

Post-execution



Action



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

DETECT

Threat Hunting







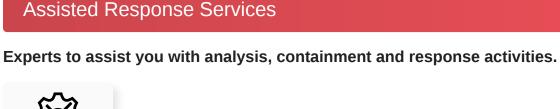


Develop containment techniques to mitigate impacts of security events: Automated Response

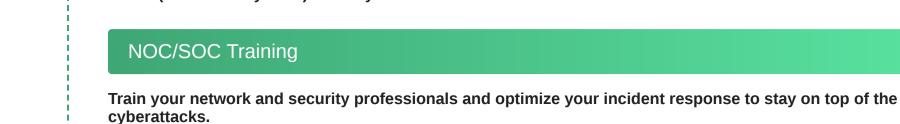
RESPOND

Services that can automatically respond to this outbreak.

FortiXDR



Incident Response

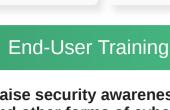


NOC/SOC Training

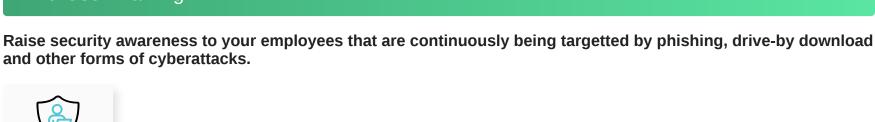
(and recovery from) security incidents:

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for



NSE Training



Response

Readiness

Awareness & **Training**



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

Vulnerability Management

Attack Surface Hardening

Security Rating



FortiEDR

https://www.cisa.gov/uscert/ncas/current-activity/2022/06/02/atlassian-releases-security-updates-confluence-server-and-

data

Additional Resources

https://www.volexity.com/blog/2022/06/02/zero-day-exploitation-of-atlassian-confluence/ 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

CISA

Volexity

Hacker News

