Atlassian Confluence and JIRA Server **Vulnerabilities**

High target vulnerabilities leading to information disclosure.

https://jira.atlassian.com/browse/JRASERVER-72695 CVEs: CVE-2021-26085, CVE-2021-26086

According to FortiGuard Labs researcher, the two vulnerabilities could eventually lead to information disclosure. The CVE-2021-26085 for Atlassian Confluence Server could allow remote attackers to view restricted resources via a Pre-Authorization Arbitrary File Read vulnerability in the /s/ endpoint. While, the CVE-2021-26086 for Atlassian Jira Server and Data Center could allow remote attackers to read particular files via a path traversal vulnerability in the /WEB-INF/web.xml endpoint.

Background

Atlassian released the advisory for CVE-2021-26085 and CVE-2021-26086 respectively on July 21 and August 21, 2021. Both CVEs has a Medium severity base score of 5.3, however software/server versions should be upgraded to correct and required versions if not already been upgraded as recommended by the vendor.

Announced

March 28, 2022: CVE-2021-26085 is added to CISA's Known Exploited Vulnerabilities Catalog.

Latest Developments

Based on the FortiGuard telemetries, the two CVEs have been a popular target for attackers. The statistics shows considerable high amount of attack detections which sometimes reaches up to 15,000 devices per day. The detected attacks are blocked by the FortiGuard IPS signature. "Atlassian.Server.S.Endpoint.Information.Disclosure"

PROTECT

events:

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

Weaponization

Reconnaissance

Delivery

IPS

Exploitation

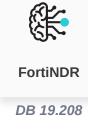
Detect and block attack attempts related to CVE-2021-26085 and CVE-2021-26086



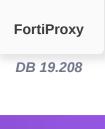
DB 19.208



DB 19.208





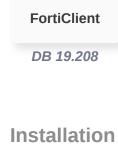


Web App Security

Detect and block attack attempts related to CVE-2021-26085



FortiWeb



Action

C2

DETECT

alert and generate reports:

Outbreak Detection

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











FortiSIEM

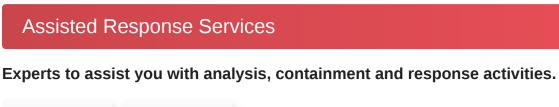
FortiSIEM

DB 310

Automated Response Services that can automatically respond to this outbreak.

RESPOND

Develop containment techniques to mitigate impacts of security events:



FortiXDR

FortiRecon: Response ACI

RECOVER



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

Security readiness and awareness training for SOC teams, InfoSec and general employees.

IDENTIFY

Response Readiness

Identify processes and assets that need protection: Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.



Security



FortiRecon:

EASM



https://www.fortiguard.com/encyclopedia/ips/50857

https://jira.atlassian.com/browse/JRASERVER-72695

Additional Resources

FortiDAST

Atlassian Advisory

IPS Signature Encyclopedia

Atlassian Advisory

https://jira.atlassian.com/browse/CONFSERVER-67893

Learn more about FortiGuard Outbreak Alerts



