Confluence enterprise servers targeted with recent vulnerability

therecord.media/confluence-enterprise-servers-targeted-with-recent-vulnerability/

September 1, 2021

Image: Atlassian, Pierre-Axel Cotteret

A major vulnerability in Confluence's team collaboration server software is currently on the cusp of widespread abuse after mass scanning and initial exploitation was spotted this week.

Tracked as **CVE-2021-26084**, the vulnerability impacts Confluence Server and Confluence Data Center software that's usually installed on Confluence self-hosted project management, wiki, and team collaboration platforms.

Under the hood, the vulnerability resides in OGNL (Object-Graph Navigation Language), a simple scripting language for interacting with Java code, the underlying technology in which most Confluence software has been written.

When it released patches on August 25, last week, Atlassian, the company that owns the Confluence software family, said the vulnerability could be exploited by threat actors to bypass authentication and inject malicious OGNL commands that allow them to take over unpatched systems.

As a result, the vulnerability was assigned a severity score of 9.8 out of a maximum of 10, as it allowed remote exploitation over the internet and because the complexity of developing a weaponized exploit was considered low.

Exploitation starts a week after patches

On Tuesday, Vietnamese security researcher Tuan Anh Nguyen said that mass scans for Confluence servers are currently underway, with attackers and professional bug bounty hunters probing Confluence systems for functions vulnerable to CVE-2021-26084 attacks.

> About CVE-2021-26084, Block endpoint /pages/createpage-entervariables.action
> If you can't patch your server. The attacker can exploit without authentication although signup is disabled by default
> Mass scan already start and bug bounty hunters are farming it 🙂#RCE #Confluence pic.twitter.com/C0JfIEYPhb
>
> — Tuan Anh Nguyen 🇻🇳 (@haxor31337) August 31, 2021

Soon after mass exploitation was spotted in the wild, two security researchers, Rahul Maini and Harsh Jaiswal, also published an in-depth explanation of the bug on GitHub, which also included several proof-of-concept payloads.

In a tweet, Maini described the process of developing the CVE-2021-26084 exploit as "relatively simpler than expected," effectively confirming why the bug received its high 9.8 severity score.

> Just did Atlassian Confluence UnAuth RCE CVE-2021-26084 along with @rootxharsh.
> It was relatively simpler than expected 😀 pic.twitter.com/7hpHt76AES
>
> — Rahul Maini (@iamnoooob) August 28, 2021

With Confluence being a wildly popular team collaboration software inside some of the world's largest corporations, and with the CVE-2021-26084 vulnerability being extremely powerful from a threat actor's perspective, attacks from criminal groups are expected to ramp up in the following days.

Confluence bugs have been widely weaponized before, so a similar exploitation pattern is expected this time as well.

On its website, Atlassian claims that Confluence is used by more than 60,000 customers, including the likes of Audi, Hubspot, NASA, LinkedIn, Twilio, and Docker.

Tags

- Atlassian
- Confluence
- CVE-2021-26084
- exploit
- exploitation
- proof-of-concept

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.