Contrast SECURITY

Confluence CVE-2021-26084: What You Should Know

On August 25, Atlassian released security updates to address a remote code execution vulnerability (CVE-2021-26084) affecting some versions of Confluence Server or Data Center software.[1]

As of September 3, widespread exploitation of the CVE-2021-26084 was being detected in the wild—prompting the U.S. federal government to issue an alert for Confluence users to update their systems without delay.[2]

What We Know

As of this writing, the impact of the mass attacks since Atlassian's disclosure (i.e., significant breach events) remains unknown. Here are some things that we do know:

- The vulnerability. CVE-2021-26084 is an Object-Graph Navigation Language (OGNL) injection vulnerability that allows an unauthenticated attacker to execute arbitrary code on a Confluence Server or Data Center instance. This vulnerability was originally discovered in late July by a researcher participating in Atlassian's public bug bounty program.[3] The vulnerability received a CVSS score of 9.8 out of 10 due to its high-risk exposure and the ubiquitous nature of the Confluence software.

- Attack methodology. Bad actors can exploit the vulnerability to inject malicious OGNL commands leading to full remote code execution (RCE). This gives the attacker full access to the Confluence server—including data, tickets, attachments, and keys. Opportunities for lateral movement beyond the breached server are also possible.

- Victims. While major instances of a successful breach occurring as a result of CVE-2021-26084 have not been reported to date, there have been widespread detections of public exploits and honeypots being hit.[4] For example, an infrastructure team at Jenkins reported a deprecated Confluence server suffered a successful attack, without any major consequences.[5]

Recommendations

The first order of business for any organization using a vulnerable version of Confluence Server or Data Center is for them to immediately apply the appropriate patch from Atlassian. While unknown/undisclosed threats do carry some risk, the critical window for any CVE (including CVE-2021-26084) comes immediately after the announcement is made. Once attackers are alerted to a CVE, they apply tremendous pressure (including automated tools) to seek out and exploit any organizations that may be slow to patch their vulnerable systems. In this case, nine days after Atlassian released its patches for vulnerable Confluence systems, large numbers of attacks were still occurring in the wild.

Contrast customers have a distinct advantage over organizations employing the more error-prone, signature-based web application firewall (WAF)-only defenses—particularly in the case of OGNL attacks. In the event an attacker targets an unknown or newly disclosed vulnerability to bypass a WAF, Contrast Protect automatically provides aircover to stop these sorts of attacks. Contrast's OGNL protection rule automatically blocks CVE-2021-26084 right out of the box.

Contrast SECURITY

Organizations that currently only use a WAF for application protection should augment their defenses with an instrumentation-based solution that provides runtime observability, such as Contrast Protect, to help ensure seamless protection against all unpatched vulnerabilities—both known and unknown.

Could a WAF Block a CVE-2021-26084 Attack?

In theory, the answer is "Yes." However, one researcher already documented how easy it was for them to bypass a WAF and then successfully exploit this vulnerability.[6] While WAFs depend on previously disclosed CVE signature detection to block exploits at the application perimeter, Contrast's approach observes the application runtime inside the code itself. Instrumentation-based visibility allows Contrast Protect to prevent injection attacks in real time.

Contrast Blocks All OGNL Injection Attacks

Not only would Contrast find and stop an attack against this particular CVE, Contrast blocks all OGNL injection attacks—such as the one that caused the catastrophic Equifax breach a few years ago.[7]

[1] "Confluence Server Webwork OGNL injection - CVE-2021-26084," Jira, accessed September 8, 2021.
[2] "Atlassian Releases Security Updates for Confluence Server and Data Center," Cybersecurity & Infrastructure Security Agency, September 3, 2021.
[3] "Confluence Server Webwork OGNL Injection (CVE 2021-26084) Exploited in the Wild," Bugcrowd, September 2, 2021.
[4] Lucian Constantin, "Critical flaw in Atlassian Confluence actively exploited," CSO, September 3, 2021.
[5] Mark Waite and R. Tyler Croy, "Jenkins project Confluence instance attacked," Jenkins, September 4, 2021.
[6] "CVE-2021-26084 Remote Code Execution on Confluence Servers," GitHub, accessed September 9, 2021.
[7] David Pitt, "Could the Equifax Hack Have Been Prevented by a Microservices Architecture?," DZone, October 2, 2017.

240 3rd Street
2nd Floor
Los Altos, CA 94022
Phone: 888.371.1333
Fax: 650.397.4133

Contrast SECURITY

contrastsecurity.com