Atlassian Confluence RCE: Critical Vulnerability

https://campus.barracuda.com/doc/97517657/

This article provides information on recently discovered Atlassian Confluence RCE vulnerability CVE-2022-26134. The vulnerability is carried out by an unauthenticated remote code execution in Confluence Server and Data Center.

The following table provides key information about the vulnerability:

Vulnerability	Pattern	Attack Definition Version	Release Date	Notes
CVE-2022-26134	RCE-OGNL	Will be updated	03 June 2022	First release

CVE-2022-26134

Description

Atlassian Confluence is a tool that provides collaborative documentation. The CVE-2022-26134 vulnerability was discovered on 2 June 2022, and in a week's time the vulnerability was used by various threat actors in assaults, and malicious actors became aware of it.

The vulnerability allows unauthenticated, remote attackers to create new administrative accounts, execute privileged commands, and can in turn seize the control of the servers.

Different methodologies were used to create various exploits to construct reverse shells, execute forced DNS requests, gather data, and create new administrative accounts.

The Barracuda WAF/WaaS/ADC is not affected by this vulnerability.

CVE Number	Commonly known/ associated as	Criticality & CVSS Score	Exploit Type	Software Firmware Version	Atlassian Cloud hosted	Barracuda WAF Affected
CVE-2022-26134	Atlassian Confluence RCE	Zero-Day Critical	RCE OGNL Injection	Confluence Server and Data Center versions after 1.3.0 are affected.	Application hosted on Atlassian cloud is not affected.	NO

Exploit

Threat actors can use a specially crafted HTTP request including the code that would run on a vulnerable server located in the URI and could result in a complete domain takeover.

The vulnerability is an Object-Graph Navigation Language (OGNL) injection.

Mitigations

The PoCs that have emerged so far are being blocked by the default Barracuda WAF signatures. It is recommended that you keep the os-command-injection-medium and *python-signatures* enabled when monitoring possible false positives.

On the Barracuda WAF, you can also manually perform the following configuration changes to protect against this vulnerability:

Barracuda WAF Manual Mitigation Configuration:

1. Create an ADR (Allow\Deny Rule) with the following values on the **WEBSITES > Allow/Deny/Redirect** page, **URL: Allow/Deny/Redirect Rules** section.
    1. **URL Match** = /*
    2. **Host Match** = *
    3. **Extended Match** = (URI co ${)
    4. **Action** = DENY

    OR

2. Create a custom pattern with pattern-regex **\$\{** on the **ADVANCED > Libraries** page, **Attack Types** section. Go to the **SECURITY POLICIES > URL Protection** page and select the pattern under **Custom Blocked Attack Types**.

This may result in some false positives, depending on how the application names other parameters. Accordingly, administrators can create the pattern initially in the **Passive** mode and review the generated Web Firewall Logs.

After evaluating the CVE, Barracuda Networks will publish the definition updates.

Recommendation

Users of affected versions should upgrade to the version as per the list published by the vendor. No other steps are necessary:

Vendor Advisory :
https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html

Atlassian has released the fixed version list for Atlassian confluence users.

- 7.4.17
- 7.13.7
- 7.14.3
- 7.15.2
- 7.16.4
- 7.17.4
- 7.18.1

Related articles:

- https://cyberint.com/blog/research/cve-2022-26134/
- https://www.bleepingcomputer.com/news/security/critical-atlassian-confluence-zero-day-actively-used-in-attacks/
- https://nvd.nist.gov/vuln/detail/CVE-2022-26134
- https://securityaffairs.co/wordpress/131961/hacking/atlassian-cve-2022-26134-rce-poc.html
- https://www.itechpost.com/articles/111142/20220606/atlassian-confluence-cve-2022-26134-vulnerability-proof-concept-exploits-released.htm