Censys

CVE-2021-26084: Confluenza

Mark Ellzey Senior Security Researcher
All posts by Mark Ellzey

Posted on September 2, 2021

Back to All Posts

Updates

- ***09-03-2021***: 11,689 Vulnerable Confluence servers scanned on 09-02-2021.
- ***09-05-2021***: 8,597 Vulnerable Confluence servers scanned on 09-04-2021.

Introduction

Confluence is a widely deployed Wiki service used primarily in collaborative corporate environments. It has become the defacto standard for enterprise documentation over the last decade and is developed and licensed by Atlassian Corporation. While the majority of users run the managed service, many companies opt to deploy the software on-prem.

What is the Issue?

On August 25th, a vulnerability in Atlassian's Confluence software was made public. A security researcher named SnowyOwl (Benny Jacob) found that an unauthenticated user could run arbitrary code by targetting HTML fields interpreted and rendered by the Object-Graph Navigation Language (OGNL). Yes, that is the same class of vulnerability used in the Equifax breach back in 2017.

The good news is that there were sanity checks in place to make sure that haxors couldn't execute malicious code. The bad news is that those checks did not correctly escape Unicode encoded characters, and the statically defined denylist of "unwanted" code definitions was not enough. With a bit of elbow grease and time, SnowyOwl was able to break through all the Confluence defenses and handed us all this hot mess. Thanks, SnowyOwl.

“12,876 individual IPv4 hosts are running an exploitable version”

Just days before this vulnerability was made public, our historical data showed that the internet had over 14,637 exposed and vulnerable Confluence servers. Compare that to the current day, September 1st, where **Censys identified 14,701 services** that self-identified as a Confluence server, and of those, **13,596 ports and 12,876 individual IPv4 hosts** are running an exploitable version of the software.

Censys was able to identify these vulnerable Confluence servers using a few data points found in the HTTP response from a running server:

- The existence of an `X-Confluence-Request-Time` response header.
- The value of the HTML meta tag: `ajs-version-number`

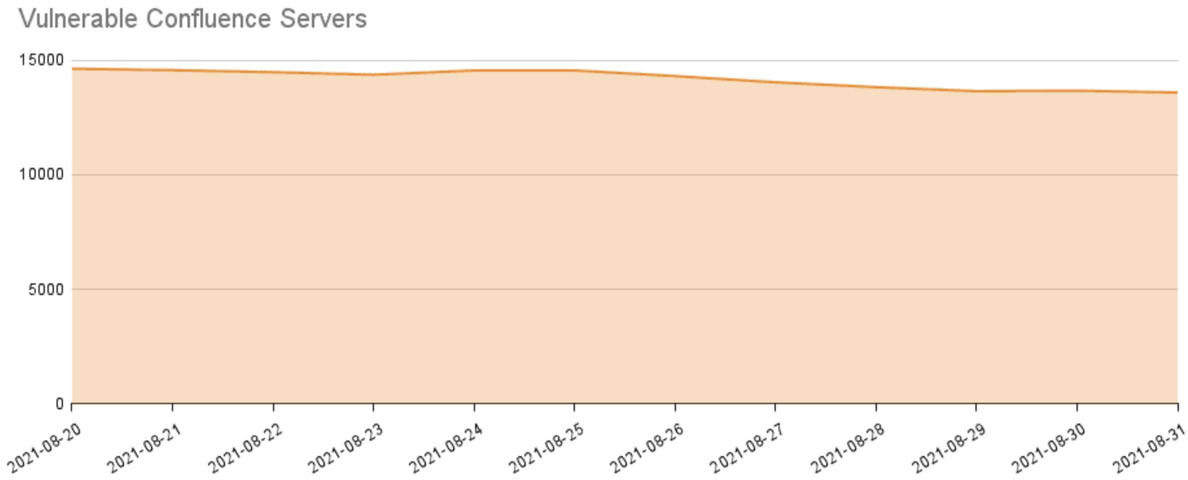
Curl output:

```
$ curl -v 'localhost:8090/login.action'
* Connected to localhost (::1) port 8090 (#0)
> GET /login.action HTTP/1.1
> Host: localhost:8090
> User-Agent: curl/7.74.0
> Accept: */*
>
< HTTP/1.1 200
< Cache-Control: no-store
< Expires: Thu, 01 Jan 1970 00:00:00 GMT
< X-Confluence-Request-Time: 1630540011363
< X-XSS-Protection: 1; mode=block
< X-Content-Type-Options: nosniff
< X-Frame-Options: SAMEORIGIN
< Content-Security-Policy: frame-ancestors 'self'
< X-Accel-Buffering: no
< Content-Type: text/html;charset=UTF-8
< Transfer-Encoding: chunked
< Date: Wed, 01 Sep 2021 23:46:51 GMT

.... snip ....

<meta name="ajs-use-keyboard-shortcuts" content="true">
<meta name="ajs-discovered-plugin-features" content="$discoveredList">
<meta name="ajs-keyboardshortcut-hash"
content="14df3a3aac8b39c774b75ab7150d0558">
<meta name="ajs-team-calendars-display-time-format"
content="displayTimeFormat12">
<meta name="ajs-is-confluence-admin" content="false">
<meta name="ajs-connection-timeout" content="10000">
<meta name="ajs-context-path" content="">
<meta name="ajs-base-url" content="http://localhost:8090">
<meta name="ajs-version-number" content="7.13.0">
<meta name="ajs-build-number" content="8703">
<meta name="ajs-remote-user" content="">
<meta name="ajs-remote-user-key" content="">
```

As news of this vulnerability spreads, Censys has seen little movement in remediating this vulnerability on a global scale. Since the public release of the exposure, only 1,041 instances have seen a version change to a non-vulnerable version. Below is a graph displaying the number of vulnerable instances by date.



Are we fully patched yet?

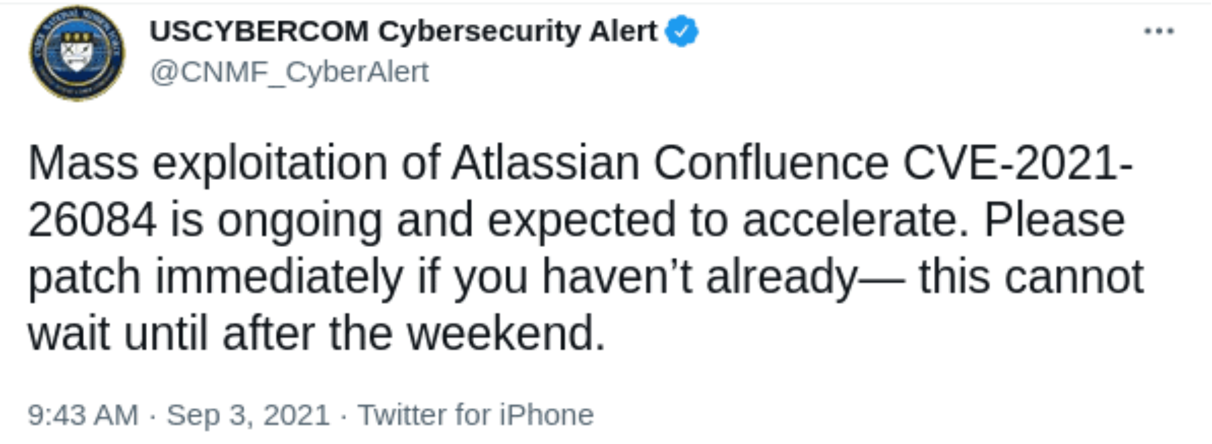
Atlassian, the owners of the Confluence software, have done a bang-up job detailing each specific version that is vulnerable to this exploit on their website. Below is a table that supplements Atlassian's vulnerable-version table with a count of services Censys has identified.

Affected Versions	**Count**
All 4.x.x versions	69
All 5.x.x versions	626
All 6.0.x versions	70
All 6.1.x versions	44
All 6.2.x versions	50
All 6.3.x versions	200
All 6.4.x versions	102
All 6.5.x versions	20
All 6.6.x versions	92
All 6.7.x versions	231
All 6.8.x versions	101
All 6.9.x versions	149
All 6.10.x versions	73
All 6.11.x versions	39
All 6.12.x versions	128
All 6.13.x versions **before** 6.13.23	541
All 6.14.x versions	266
All 6.15.x versions	2351
All 7.0.x versions	448
All 7.1.x versions	388
All 7.2.x versions	623
All 7.3.x versions	844

Affected Versions	Count
All 7.4.x versions **before** 7.4.11	2419
All 7.5.x versions	375
All 7.6.x versions	370
All 7.7.x versions	308
All 7.8.x versions	341
All 7.9.x versions	409
All 7.10.x versions	402
All 7.11.x versions **before** 7.11.6	515
All 7.12.x versions **before** 7.12.5	947

Update: 09-03-2021

Mass exploitation of this vulnerability is currently underway.

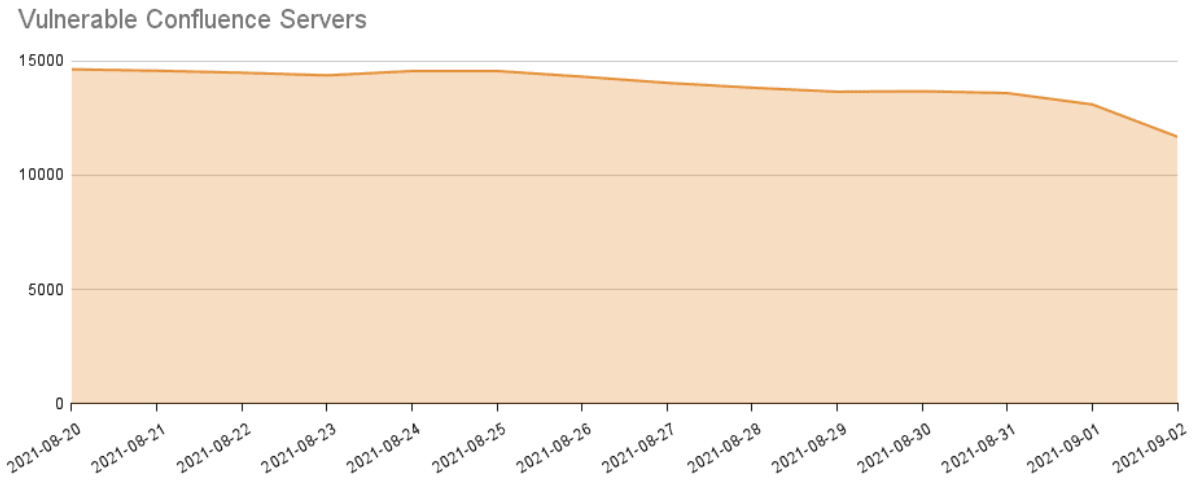


USCYBERCOM Cybersecurity Alert
@CNMF_CyberAlert

Mass exploitation of Atlassian Confluence CVE-2021-26084 is ongoing and expected to accelerate. Please patch immediately if you haven’t already— this cannot wait until after the weekend.

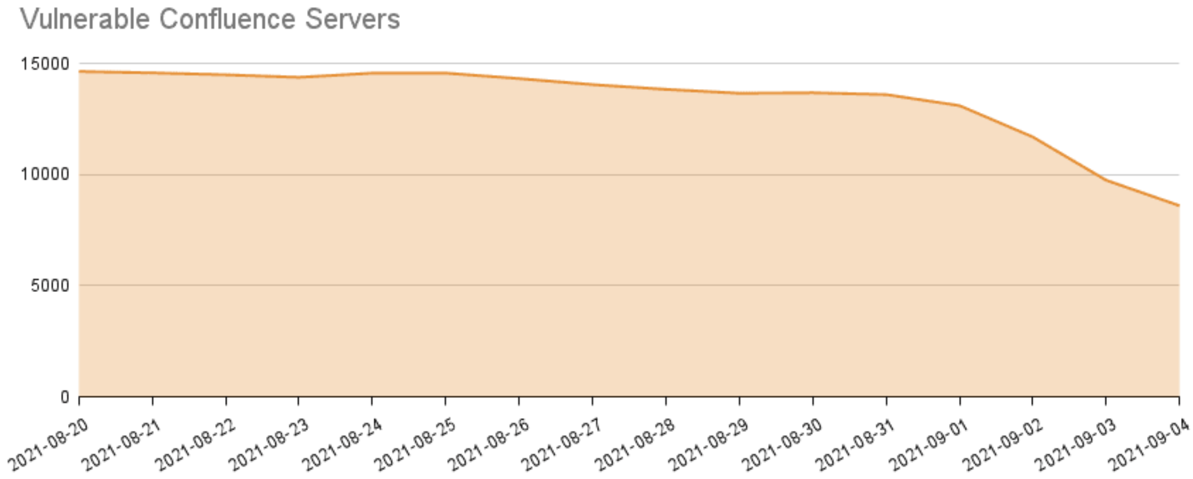
9:43 AM · Sep 3, 2021 · Twitter for iPhone

Over the last few days, Censys has seen a small shift in the number of vulnerable servers still running on the public internet. On August 31st, Censys identified 13,596 vulnerable Confluence instances, while **on September 02, that number has decreased to 11,689 vulnerable instances.**



Update: 09-05-2021

Over the last few days, **Censys observed the number of vulnerable Confluence instances drop from 11,689 to 8,597 – a 3,092 difference since September 02**, and a total of 5,965 since the vulnerability was made public on August 25th.



Why does it matter?

An attacker can leverage this vulnerability to execute any command with the same permissions as the user-id running the service. An attacker can then use this access to gain elevated administrative permissions if the host has unpatched local vulnerabilities.

There is no way to put this lightly: this is bad. Initially, Atlassian stated this was only exploitable if a user had a valid account on the system; this was found to be incorrect and the advisory was updated today to reflect the new information. It's only a matter of time before we start seeing active exploitation in the wild as there have already been working exploits found scattered about.

What do I do about it?

Since a mass-exploitation event is ongoing, Censys has decided to release a search query for finding open Confluence services. Readers should note that the results returned by public search will include both patched and unpatched services:

- same_service(services.http.response.body: `<meta name="ajs-version-number"` AND services.http.response.headers.unknown.name: "X-Confluence-Request-Time")

- Censys ASM customers have been notified via email for any hosts that have been identified as vulnerable.
- Follow the instructions on Atlassian's webpage about this vulnerability.
- **Upgrade to version 7.13.0 (LTS) or higher**.
    - For **6.13.x versions** which cannot be upgraded to 7.13.0, **upgrade to version 6.13.23**
    - For **7.4.x** versions which cannot be upgraded to 7.13.0, **upgrade to version 7.4.11**

    - For **7.11.x** versions which cannot be upgraded to 7.13.0, **upgrade to version 7.11.6**
    - For **7.12.x** versions which cannot be upgraded to 7.13.0, **upgrade to version 7.12.5**
- If you are unable to upgrade to any of the prior versions, Atlassian has created a script that attempts to mitigate the issue:
    - Linux Mitigation Script
    - Microsoft Windows Mitigation Script

Known Exploits

- https://www.exploit-db.com/exploits/50243
- https://github.com/alt3kx/CVE-2021-26084_PoC

References

- CVE-2021-26084 at NIST
- Atlassian's Advisory
- Detailed Writeup
- Proof of Concept

Please feel free to email press@censys.io with any questions.