HIGH

Search by package name or CVE

Arbitrary File Write via Archive Extraction (Zip Slip)

Affecting elfinder.netcore package, versions [0,]

INTRODUCED: 20 AUG 2021 CVE-2021-23427 ? CWE-29 ? FIRST ADDED BY SNYK

Share

How to fix?

There is no fixed version for `elFinder.NetCore` .

Overview

elFinder.NetCore is a file manager for Web.

Affected versions of this package are vulnerable to Arbitrary File Write via Archive Extraction (Zip Slip). The `ExtractAsync` function within the `FileSystem` is vulnerable to arbitrary extraction due to insufficient validation.

PoC

```
* Upload the genearted evil.zip to the server * extract the evil.zip file in elfinder * You now should fine a file in the
/tmp/ directory
```

Details

It is exploited using a specially crafted zip archive, that holds path traversal filenames. When exploited, a filename in a malicious archive is concatenated to the target extraction directory, which results in the final path ending up outside of the target folder. For instance, a zip may hold a file with a "../../file.exe" location and thus break out of the target folder. If an executable or a configuration file is overwritten with a file containing malicious code, the problem can turn into an arbitrary code execution issue quite easily.

The following is an example of a zip archive with one benign file and one malicious file. Extracting the malicous file will result in traversing out of the target folder, ending up in `/root/.ssh/` overwriting the `authorized_keys` file:

```
+2018-04-15 22:04:29 ..... 19 19 good.txt
```

```
+2018-04-15 22:04:42 ..... 20 20 ../../../../../../root/.ssh/authorized_keys
```

References

- Vulnerable Code

Snyk CVSS

Exploit Maturity	Mature ?
Attack Complexity	Low ?
Confidentiality	HIGH ?

See more

› NVD 9.8 CRITICAL

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk ID	SNYK-DOTNET-ELFINDERNETCORE-1567778
Published	20 Aug 2021
Disclosed	20 Aug 2021
Credit	Timo Müller

Report a new vulnerability

Found a mistake?

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT