Arbitrary File Write via Archive Extraction (Zip Slip)

Affecting github.com/sassoftware/go-rpmutils/cpio package, versions **<0.1.0**

INTRODUCED: 27 MAY 2020 CVE-2020-7667 CWE-22 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `github.com/sassoftware/go-rpmutils/cpio` to version 0.1.0 or higher.

Overview

github.com/sassoftware/go-rpmutils/cpio is a package for parsing and extracting content from RPM files.

Affected versions of this package are vulnerable to Arbitrary File Write via Archive Extraction (Zip Slip). The CPIO extraction functionality doesn't sanitize the paths of the archived files for leading and non-leading ".." which leads in file extraction outside of the current directory.

Note: the fixing commit was applied to all affected versions which were re-released.

PoC by Georgios Gkitsas of Snyk Security Team

Having a modified `relative.cpio` that includes relative paths:

```
package main
import ( cpio "github.com/sassoftware/go-rpmutils/cpio" "os" "testing/iotest" "fmt" )

func main() { file := "relative.cpio"

  f, err := os.Open(file) if err != nil { fmt.Println(err) } hf := iotest.HalfReader(f) if err := cpio.Extract(hf, &amp;quot;.&amp;quot;); err
  != nil { fmt.Println(err) }


}
```

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

- GitHub Fixing Commit

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	Low
Integrity	HIGH

See more

NVD 7.5 HIGH

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 Learn

Learn about Arbitrary File Write via Archive Extraction (Zip Slip) vulnerabilities in an interactive lesson.

Start learning

Snyk ID	SNYK-GOLANG-GITHUBCOMSASSOFTWAREGORPMUTILSCPIO-570427
Published	5 Jun 2020
Disclosed	27 May 2020
Credit	Georgios Gkitsas of Snyk Security Team

Report a new vulnerability | Found a mistake?