# **snyk** Vulnerability DB

Snyk Vulnerability Database > Go > github.com/unknwon/cae/zip

# Arbitrary File Write via Archive Extraction (Zip Slip)

Affecting github.com/unknwon/cae/zip package, versions <1.0.1



Proof of concept @

Snyk CVSS

**Exploit Maturity** 

# INTRODUCED: 26 MAY 2020 CVE-2020-7664 © CWE-22 © FIRST ADDED BY SNYK How to fix? Upgrade github.com/unknwon/cae/zip to version 1.0.1 or higher.

#### Overview

 $github.com/unknwon/cae/zip\ is\ a\ package\ that\ provides\ archiving\ functionality\ for\ \ .zip\ archives.$ 

Affected versions of this package are vulnerable to Arbitrary File Write via Archive Extraction (Zip Slip). The ExtractTo function doesn't securely escape file paths in zip archives which include leading or non-leading "..". This allows an attacker to add or replace files system-wide

## PoC by Georgios Gkitsas

```
package main
import ( cae_zip "github.com/unknwon/cae/zip" )
func main() { file := "relative.zip" z, _ := cae_zip.Open(file) z.ExtractTo(".") }
```

where "relative.zip" is a zip archive that includes a leading/non-leading ".." in at least one file path.

## 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.

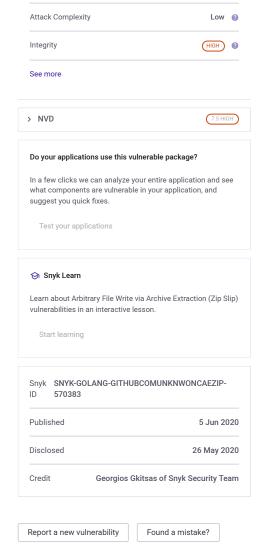
The following is an example of a zip archive with one benign file and one malicious file. Extracting the malicous file will result in traversing out of the target folder, ending up in /root/.ssh/ overwriting the authorized\_keys file:

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

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

## References

GitHub Commit



PRODUCT
Snyk Open Source
Snyk Code
Snyk Container
Snyk Infrastructure as Code
Test with Github
Test with CLI
RESOURCES
Vulnerability DB

COMPANY
About
Jobs
Contact
Policies
Do Not Sell My Personal Information

CONTACT US
Support
Report a new vuln
Press Kit

FIND US ONLINE

TRACK OUR DEVELOPMENT





© 2022 Snyk Limited

Disclosed Vulnerabilities

Blog FAQs

Events

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.