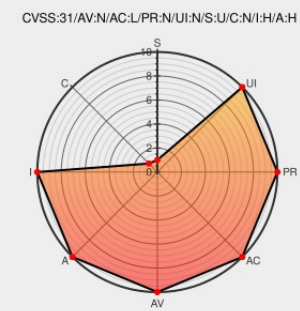
CVE-2018-25046

Published on: Not Yet Published

Last Modified on: 06/08/2023 09:15:00 PM UTC

CVE-2018-25046

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Archiver from Cloudfoundry contain the following vulnerability:

Due to improper path sanitization, archives containing relative file paths can cause files to be written (or overwritten) outside of the target directory.

CVE-2018-25046 has been assigned by security@golang.org to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **code.cloudfoundry.org/archiver** - **code.cloudfoundry.org/archiver/extractor** version **< 0.0.0-20180523222229-09b5706aa936**

CVSS3 Score: 9.1 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	HIGH

CVE References

Description	Tags	Link
GO-2020-0025 - Go Packages	pkg.go.dev, text/html	MISC pkg.go.dev/vuln/GO-2020-0025
Zip Slip Vulnerability | Snyk	snyk.io, text/html	MISC snyk.io/research/zip-slip-vulnerability
Refactored the path resolution to use securejoin · cloudfoundry/archiver@09b5706 · GitHub	github.com, text/html	MISC github.com/cloudfoundry/archiver/commit/09b5706aa9367972c09144a450bb4523049ee840

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cloudfoundry	Archiver	All	All	All	All

cpe:2.3:a:cloudfoundry:archiver:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→