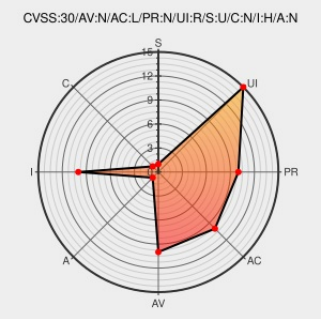
CVE-2018-1002202

Published on: 07/25/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:37 PM UTC

CVE-2018-1002202

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



Certain versions of Zip4j from Zip4j Project contain the following vulnerability:

zip4j before 1.3.3 is vulnerable to directory traversal, allowing attackers to write to arbitrary files via a ../ (dot dot slash) in a Zip archive entry that is mishandled during extraction. This vulnerability is also known as 'Zip-Slip'.

CVE-2018-1002202 has been assigned by report@snyk.io to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **zip4j** - **zip4j** version **< 1.3.3**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
GitHub - snyk/zip-slip-vulnerability: Zip Slip Vulnerability (Arbitrary file write through archive extraction)	Exploit, Third Party Advisory, github.com	MISC github.com/snyk/zip-slip-vulnerability

	text/html	
Document Display | HPE Support Center	Third Party Advisory support.hpe.com text/html	CONFIRM support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbmu03895en_us
Zip Slip Vulnerability | Snyk	Exploit Issue Tracking Patch Third Party Advisory snyk.io text/html	MISC snyk.io/research/zip-slip-vulnerability
Arbitrary File Write via Archive Extraction (Zip Slip) in net.lingala.zip4j:zip4j | Snyk	Third Party Advisory snyk.io text/html	MISC snyk.io/vuln/SNYK-JAVA-NETLINGALAZIP4J-31679

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zip4j Project	Zip4j	All	All	All	All
Application	Zip4j Project	Zip4j	All	All	All	All

cpe:2.3:a:zip4j_project:zip4j:*:*:*:*:*:*:*:*:

cpe:2.3:a:zip4j_project:zip4j:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→