

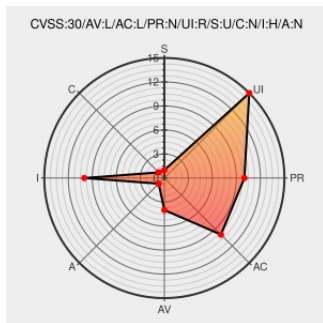


CVE-2018-1002209

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

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

CVE-2018-1002209

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Quazip](#) from [Quazip Project](#) contain the following vulnerability:

QuaZIP before 0.7.6 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-2018-1002209 has been assigned by [report@snyk.io](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **quazip** - **quazip** version < 0.7.6

CVSS3 Score: **5.5 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
quazip/NEWS.txt at 0.7.6 · stachenov/quazip · GitHub	Release Notes github.com text/html	CONFIRM github.com/stachenov/quazip/blob/0.7.6/NEWS.txt

Fixed the Zip Slip vulnerability in JICompress · stachenov/quazip@5d2fc16 · GitHub

Patch

github.com

text/html

CONFIRM

github.com/stachenov/quazip/commit/5d2fc16a1976e5bf78d2927b012f67a2ae047a98

GitHub - snyk/zip-slip-vulnerability: Zip Slip Vulnerability (Arbitrary file write through archive extraction)

Third Party Advisory

github.com

text/html

MISC

github.com/snyk/zip-slip-vulnerability

Zip Slip Vulnerability | Snyk

Third Party Advisory

snyk.io

text/html

MISC

snyk.io/research/zip-slip-vulnerability

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that 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	Quazip Project	Quazip	All	All	All	All
Application	Quazip Project	Quazip	All	All	All	All

cpe:2.3:a:quazip_project:quazip:*****::

cpe:2.3:a:quazip_project:quazip:*****::

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →