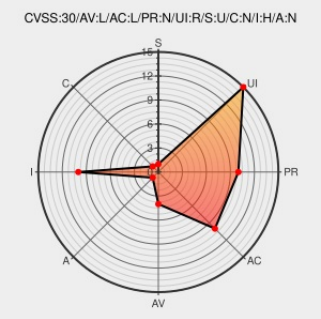
CVE-2018-1002205

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

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

CVE-2018-1002205

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



Certain versions of Dotnetzip.semverd from Dotnetzip.semverd Project contain the following vulnerability:

DotNetZip.Semvered before 1.11.0 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-2018-1002205 has been assigned by report@snyk.io to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **DotNetZip** - **DotNetZip.Semvered** version **< 1.11.0**

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
Merge pull request #121 from shana/bugs/relative-paths · haf/DotNetZip.Semverd@55d2c13	Patch github.com text/html	CONFIRM github.com/haf/DotNetZip.Semverd/commit/55d2c13c0cc64654e18fcdd0038fdb3d7

· GitHub		
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
Arbitrary File Write via Archive Extraction (Zip Slip) in dotnetzip | Snyk	Third Party Advisory snyk.io text/html	MISC snyk.io/vuln/SNYK-DOTNET-DOTNETZIP-60245
Zip Slip Vulnerability | Snyk	Third Party Advisory snyk.io text/html	MISC snyk.io/research/zip-slip-vulnerability
Sanitize zip entry paths before extracting by shana · Pull Request #121 · haf/DotNetZip.Semverd · GitHub	Patch github.com text/html	CONFIRM github.com/haf/DotNetZip.Semverd/pull/121

Related QID Numbers

983149 Dotnet (nuget) Security Update for DotNetZip (GHSA-7378-6268-4278)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dotnetzip.semverd Project	Dotnetzip.semverd	All	All	All	All
Application	Dotnetzip.semverd Project	Dotnetzip.semverd	All	All	All	All

cpe:2.3:a:dotnetzip.semverd_project:dotnetzip.semverd:*:*:*:*:*:*:*:*:

cpe:2.3:a:dotnetzip.semverd_project:dotnetzip.semverd:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→