



CVE-2019-16760

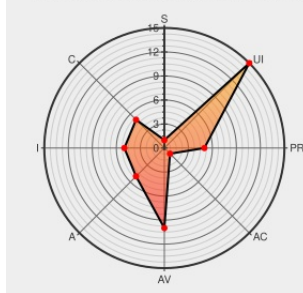
Published on: 09/30/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:48 PM UTC

CVE-2019-16760 - advisory for GHSA-phjm-8x66-qw4r

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

CVSS:31/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L



Certain versions of [Rust](#) from [Rust-lang](#) contain the following vulnerability:

Cargo prior to Rust 1.26.0 may download the wrong dependency if your package.toml file uses the `package` configuration key. Usage of the `package` key to rename dependencies in `Cargo.toml` is ignored in Rust 1.25.0 and prior. When Rust 1.25.0 and prior is used Cargo may download the wrong dependency, which could be squatted on

crates.io to be a malicious package. This not only affects manifests that you write locally yourself, but also manifests published to crates.io. Rust 1.0.0 through Rust 1.25.0 is affected by this advisory because Cargo will ignore the `package` key in manifests. Rust 1.26.0 through Rust 1.30.0 are not affected and typically will emit an error because the `package` key is unstable. Rust 1.31.0 and after are not affected because Cargo understands the `package` key. Users of the affected versions are strongly encouraged to update their compiler to the latest available one. Preventing this issue from happening requires updating your compiler to be either Rust 1.26.0 or newer. There will be no point release for Rust versions prior to 1.26.0. Users of Rust 1.19.0 to Rust 1.25.0 can instead apply linked patches to mitigate the issue.

CVE-2019-16760 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [rust](#) - cargo version < 1.26.0

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
---------------	-------------------	----------------

NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Cargo prior to Rust 1.26.0 may download the wrong dependency · Advisory · rust-lang/rust · GitHub	Exploit Third Party Advisory github.com text/html	CONFIRM github.com/rust-lang/rust/security/advisories/GHSA-phjm-8x66-qw4r
Patches for CVE-2019-16760 · GitHub	Patch Third Party Advisory gist.github.com text/html	MISC gist.github.com/pietroalbini/0d293b24a44babbe6187e06eebd4992
oss-security - CVE-2019-16760: Cargo prior to Rust 1.26.0 may download the wrong dependency	www.openwall.com text/html	MLIST [oss-security] 20191008 CVE-2019-16760: Cargo prior to Rust 1.26.0 may download the wrong dependency
Google Groups	Exploit Mailing List Third Party Advisory groups.google.com text/html	MISC groups.google.com/forum/#!topic/rustlang-security-announcements/rVQ5e3TDnpQ

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.

Related QID Numbers

[501241](#) Alpine Linux Security Update for rust

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rust-lang	Rust	All	All	All	All
Application	Rust-lang	Rust	All	All	All	All
cpe:2.3:a:rust-lang:rust:*.***:*.***:.*						
cpe:2.3:a:rust-lang:rust:*.***:*.***:.*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)