



CVE-2021-27378

Published on: 02/17/2021 12:00:00 AM UTC

Last Modified on: 07/12/2022 05:42:00 PM UTC

CVE-2021-27378

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

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

An issue was discovered in the rand_core crate before 0.6.2 for Rust. Because read_u32_into and read_u64_into mishandle certain buffer-length checks, a random number generator may be seeded with too little data.

CVE-2021-27378 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
About RustSec › RustSec Advisory Database	Third Party Advisory rustsec.org text/html	MISC rustsec.org/advisories/RUSTSEC-2021-0023.html

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

905163 Common Base Linux Mariner (CBL-Mariner) Security Update for libsvg2 (12517)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rand Core Project	Rand Core	All	All	All	All
Application	Rand Core Project	Rand Core	All	All	All	All
cpe:2.3:a:rand_core_project:rand_core:*:*:*:*:rust:*:*:						
cpe:2.3:a:rand_core_project:rand_core:*:*:*:*:rust:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)