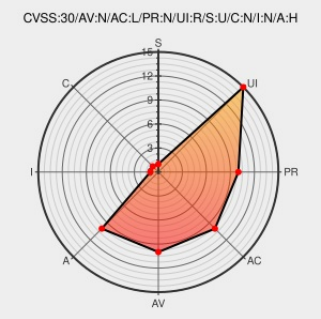
CVE-2019-1010182

Published on: 07/25/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:57 PM UTC

CVE-2019-1010182

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



Certain versions of Yaml-rust from Yaml-rust Project contain the following vulnerability:

yaml-rust 0.4.0 and earlier is affected by: Uncontrolled Recursion. The impact is: Denial of service by impossible to catch abort. The component is: YamlLoader::load_from_str function. The attack vector is: Parsing of a malicious YAML document. The fixed version is: 0.4.1 and later.

CVE-2019-1010182 has been assigned by GSD cve-assign@distributedweaknessfiling.org to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: GSD **yaml-rust** - **yaml-rust** version **0.4.0 and earlier [fixed: 0.4.1 and later]**

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	NONE	HIGH

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link

Prevent too deep recursion by xfix · Pull Request #109 · chyh1990/yaml-rust · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	MISC github.com/chyh1990/yaml-rust/pull/109

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Yaml-rust Project	Yaml-rust	All	All	All	All

cpe:2.3:a:yaml-rust_project:yaml-rust:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→