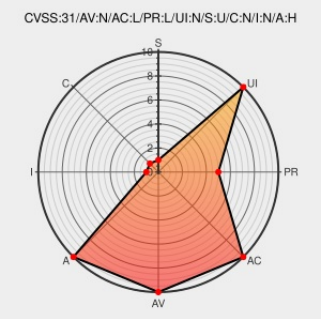
CVE-2020-5238

Published on: 07/01/2020 12:00:00 AM UTC

Last Modified on: 01/28/2023 01:44:00 AM UTC

CVE-2020-5238 - advisory for GHSA-7gc6-9qr5-hc85

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



Certain versions of Fedora from Fedoraproject contain the following vulnerability:

The table extension in GitHub Flavored Markdown before version 0.29.0.gfm.1 takes O(n * n) time to parse certain inputs. An attacker could craft a markdown table which would take an unreasonably long time to process, causing a denial of service. This issue does not affect the upstream cmark project. The issue has been fixed in version 0.29.0.gfm.1.

CVE-2020-5238 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **github** - **cmark-gfm** version **< 0.29.0.gfm.1**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link

Description	Tags	Link
[SECURITY] Fedora 32 Update: pandoc-2.7.3-4.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-1eaffe0013
Merge pull request from GHSA-7gc6-9qr5-hc85 · github/cmark-gfm@85d8952 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/github/cmark-gfm/commit/85d895289c5ab67f988ca659493a64abb5fec7b4
Denial of service in table parsing · Advisory · github/cmark-gfm · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/github/cmark-gfm/security/advisories/GHSA-7gc6-9qr5-hc85
[SECURITY] Fedora 31 Update: ghc-cmark-gfm-0.2.2-1.fc31 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-fe299b3fa3
[SECURITY] Fedora 33 Update: pandoc-citeproc-0.17.0.1-3.fc33 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-c39d7a562c

Related QID Numbers

940402 AlmaLinux Security Update for pandoc (ALSA-2021:1972)

960207 Rocky Linux Security Update for pandoc (RLSA-2021:1972)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Github Flavored Markdown Project	Github Flavored Markdown	All	All	All	All
Application	Github Flavored Markdown Project	Github Flavored Markdown	All	All	All	All

cpe:2.3:o:fedoraproject:fedora:31:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:32:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:33:*:*:*:*:*:*:*:

cpe:2.3:a:github_flavored_markdown_project:github_flavored_markdown:*:*:*:*:*:*:*:*:

cpe:2.3:a:github_flavored_markdown_project:github_flavored_markdown:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→