



CVE-2023-28631

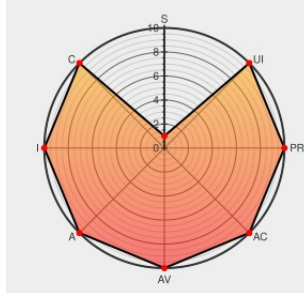
Published on: Not Yet Published

Last Modified on: 04/29/2023 07:15:00 AM UTC

CVE-2023-28631 - advisory for GHSA-5r3x-p7xx-x6q5

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

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



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

comrak is a CommonMark + GFM compatible Markdown parser and renderer written in rust. A Comrak AST can be constructed manually by a program instead of parsing a Markdown document with ``parse_document``. This AST can then be converted to HTML via ``html::format_document_with_plugins``. However, the HTML formatting code assumes that the AST is well-formed. For example, many AST notes contain ``[u8]`` fields which the formatting code assumes is valid UTF-8 data. Several bugs can be triggered if this is not the case. Version 0.17.0 contains adjustments to the AST, storing strings instead of unvalidated byte arrays. Users are advised to upgrade. Users unable to upgrade may manually validate UTF-8 correctness of all data when assigning to ``&[u8]`` and ``Vec<u8>`` fields in the AST. This issue is also tracked as ``GHSL-2023-049``.

CVE-2023-28631 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [kivikakk](#) - **comrak** version = < 0.17.0

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

CVE References

Description	Tags	Link
[SECURITY] Fedora 37 Update: rust-comrak-0.18.0-1.fc37	lists.fedoraproject.org/text/html	MISC lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OUYME2VA555X6567H7ORIQQFN4BVG6N

0.18.0-1.fc37 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 36 Update: rust-askama_shared-0.12.2-4.fc36 - package-announce - Fedora Mailing-Lists

lists.fedoraproject.org

text/html

MISC lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/VQ3UBC7LE4VPCMZBTADIBL353CH7CPVV

Attacker controlled data in AST nodes is not validated (GHSL-2023-049) · Advisory · kivikakk/comrak · GitHub

github.com

text/html

MISC github.com/kivikakk/comrak/security/advisories/GHSA-5r3x-p7xx-x6q5

Merge pull request from GHSA-5r3x-p7xx-x6q5 · kivikakk/comrak@9ff5f8d · GitHub

github.com

text/html

MISC github.com/kivikakk/comrak/commit/9ff5f8df0ac951f5742d22a72c39b89a15f5663

[SECURITY] Fedora 38 Update: rust-comrak-0.18.0-1.fc38 - package-announce - Fedora Mailing-Lists

lists.fedoraproject.org

text/html

MISC lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/PTWZWCT7KCX2KTXTLPUYZ3EHOONG4X4

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

283948

Fedora Security Update for rust (FEDORA-2023-b37722768e)

283949

Fedora Security Update for rust (FEDORA-2023-e9243281cb)

284162

Fedora Security Update for rust (FEDORA-2023-035d5910b9)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Comrak Project	Comrak	All	All	All	All
cpe:2.3:a:comrak_project:comrak:*:*:*:*:rust:*:*						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
@CVEreport	CVE-2023-28631 : comrak is a CommonMark + GFM compatible Markdown parser and renderer written in rust. A Comrak AST... twitter.com/i/web/status/1...	2023-03-28 21:12:40
/r/netcve	CVE-2023-28631	2023-03-28 21:38:42

© [CVE.report](#) 2024   |

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](#)