



CVE-2022-24803

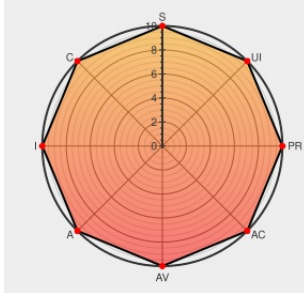
Published on: Not Yet Published

Last Modified on: 04/11/2022 08:15:00 PM UTC

CVE-2022-24803 - advisory for GHSA-v222-6mr4-qj29

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

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



Certain versions of [Asciidoctor-include-ext](#) from [Asciidoctor-include-ext Project](#) contain the following vulnerability:

Asciidoctor-include-ext is Asciidoctor's standard include processor reimplemented as an extension. Versions prior to 0.4.0, when used to render user-supplied input in AsciiDoc markup, may allow an attacker to execute arbitrary system commands on the host operating system.

This attack is possible even when `allow-uri-read` is disabled! The problem has been patched in the referenced commits.

CVE-2022-24803 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [jirutka](#) - [asciidoctor-include-ext](#) version < 0.4.0

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

CVSS2 Score: **10 - HIGH**

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

CVE References

Description	Tags	Link
-------------	------	------

Description	Tags	Link
Command Injection vulnerability in asciidoctor-include-ext · Advisory · jirutka/asciidoctor-include-ext · GitHub	github.com text/html	CONFIRM github.com/jirutka/asciidoctor-include-ext/security/advisories/GHSA-v222-6mr4-qj29
Make #read_lines code more robust, avoid using IO.open directly · jirutka/asciidoctor-include-ext@cbaccf3 · GitHub	github.com text/html	MISC github.com/jirutka/asciidoctor-include-ext/commit/cbaccf3de533cbca224bf61d0b74e4b84d41d8ee
Fix command injection vulnerability · jirutka/asciidoctor-include-ext@c7ea001 · GitHub	github.com text/html	MISC github.com/jirutka/asciidoctor-include-ext/commit/c7ea001a597c7033575342c51483dab7b87ae155

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

182675 Debian Security Update for ruby-asciidoctor-include-ext (CVE-2022-24803)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Asciidoctor-include-ext Project	Asciidoctor-include-ext	All	All	All	All
cpe:2.3:a:asciidoctor-include-ext_project:asciidoctor-include-ext:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-24803 : Asciidoctor-include-ext is Asciidoctor's standard include processor reimplemented as an extension.... twitter.com/i/web/status/1...	2022-03-31 23:34:52
/r/netcve	CVE-2022-24803	2022-04-01 00:38:35

[← 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](#)