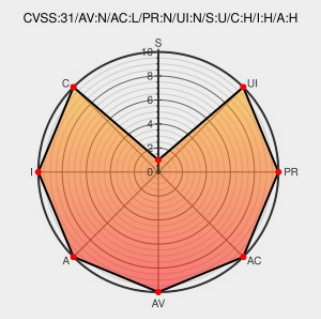
CVE-2021-28834

Published on: 03/19/2021 12:00:00 AM UTC

Last Modified on: 04/19/2021 08:39:00 PM UTC

CVE-2021-28834

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

Kramdown before 2.3.1 does not restrict Rouge formatters to the Rouge::Formatters namespace, and thus arbitrary classes can be instantiated.

CVE-2021-28834 has been assigned by 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: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
No Description Provided	lists.fedoraproject.org Inactive Link Not Archived	FEDORA FEDORA-2021-4c57a892d1
Debian -- Security Information -- DSA-	www.debian.org	DEBIAN DSA-4890

4890-1 ruby-kramdown	Depreciated Link text/html	
Restrict Rouge formatters to Rouge::Formatters namespace by stanhu · Pull Request #708 · gettalong/kramdown · GitHub	github.com text/html	MISC github.com/gettalong/kramdown/pull/708
[SECURITY] Fedora 32 Update: rubygem-kramdown-2.1.0-5.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-edc673e864
Comparing REL_2_3_0...REL_2_3_1 · gettalong/kramdown · GitHub	github.com text/html	MISC github.com/gettalong/kramdown/compare/REL_2_3_0...REL_2_3_1
Patch Kramdown syntax highlighter gem (179329b5) · Commits · GitLab.org / GitLab · GitLab	gitlab.com text/html	MISC gitlab.com/gitlab-org/gitlab/-/commit/179329b5c3c118924fb242dc449d06b4ed6ccb66
[SECURITY] Fedora 34 Update: rubygem-kramdown-2.3.1-1.fc34 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-139a6a2f9d

Related QID Numbers

178532 Debian Security Update for ruby-kramdown (DSA 4890-1)

179925 Debian Security Update for ruby-kramdown (CVE-2021-28834)

199819 Ubuntu Security Notification for kramdown Vulnerability (USN-6424-1)

281442 Fedora Security Update for rubygem (FEDORA-2021-139a6a2f9d)

281443 Fedora Security Update for rubygem (FEDORA-2021-edc673e864)

281444 Fedora Security Update for rubygem (FEDORA-2021-4c57a892d1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Application	Kramdown Project	Kramdown	All	All	All	All

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:*:*

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

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

cpe:2.3:o:fedoraproject:fedora:34:*:*:*:*:*:*:*:

cpe:2.3:a:kramdown_project:kramdown:*:*:*:*:*:ruby:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→