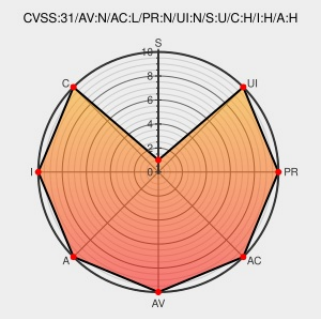
CVE-2020-14001

Published on: 07/17/2020 12:00:00 AM UTC

Last Modified on: 04/28/2022 06:57:00 PM UTC

CVE-2020-14001

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



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

The kramdown gem before 2.3.0 for Ruby processes the template option inside Kramdown documents by default, which allows unintended read access (such as template="/etc/passwd") or unintended embedded Ruby code execution (such as a string that begins with template="string://<%= `). NOTE: kramdown is used in Jekyll, GitLab Pages, GitHub Pages, and Thredded Forum.

CVE-2020-14001 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: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Pony Mail!	Mailing List Third Party Advisory	MLIST [fluo-notifications] 20200808 [GitHub] [fluo-website] ctubbsii opened a ne pull request #194: Update gems

	lists.apache.org text/html	
Home | kramdown	Vendor Advisory kramdown.gettalong.org text/html	MISC kramdown.gettalong.org
[SECURITY] Fedora 31 Update: rubygem-kramdown-1.17.0-6.fc31 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-5c70d97eca
gettalong's kramdown at master - GitHub	Third Party Advisory github.com text/html	MISC github.com/gettalong/kramdown
News | kramdown	Release Notes Vendor Advisory kramdown.gettalong.org text/html	CONFIRM kramdown.gettalong.org/news.html
Comparing REL_2_2_1...REL_2_3_0 · gettalong/kramdown · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/gettalong/kramdown/compare/REL_2_2_1...REL_2_3_0
Add option forbidden_inline_options · gettalong/kramdown@1b8fd33 · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/gettalong/kramdown/commit/1b8fd33c3120bfc6e5164b449e2c2fc9c930
Debian -- Security Information -- DSA-4743-1 ruby-kramdown	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-4743
USN-4562-1: kramdown vulnerability | Ubuntu security notices | Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-4562-1
CVE-2020-14001 Ruby Vulnerability in NetApp Products | NetApp Product Security	Third Party Advisory security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20200731-0004/
[SECURITY] [DLA 2316-1] ruby-kramdown security update	Mailing List Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20200809 [SECURITY] [DLA 2316-1] ruby-kramdc security update
kramdown | RubyGems.org | your community gem host	Third Party Advisory rubygems.org text/html	MISC rubygems.org/gems/kramdown
[SECURITY] Fedora 32 Update: rubygem-kramdown-2.1.0-3.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-f6eee9a2d3

Related QID Numbers

500997 Alpine Linux Security Update for icinga2

753492 SUSE Enterprise Linux Security Update for rubygem-kramdown (SUSE-SU-2022:3259-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Kramdown Project	Kramdown	All	All	All	All
Application	Kramdown Project	Kramdown	All	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:20.04:*:*:*:lts:*:*:*:

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

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

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

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

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

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

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

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→

CVE.report and Source URL Uptime Status status.cve.report