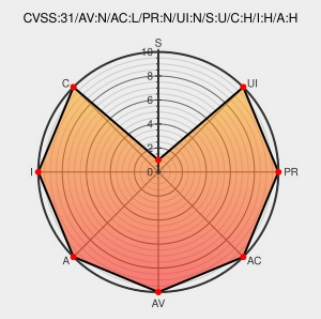
CVE-2018-11743

Published on: 06/05/2018 12:00:00 AM UTC

Last Modified on: 05/12/2022 08:11:00 PM UTC

CVE-2018-11743

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



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

The init_copy function in kernel.c in mruby 1.4.1 makes initialize_copy calls for TT_ICLASS objects, which allows attackers to cause a denial of service (mrb_hash_keys uninitialized pointer and application crash) or possibly have unspecified other impact.

CVE-2018-11743 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
Should not call `initialize_copy` for `TT_ICLASS`; fix #4027 · mruby/mruby@b64ce17 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/mruby/mruby/commit/b64ce17852b180dfeea81cf458660be41a78974d

Use of uninitialized pointer in mrb_hash_keys · Issue #4027 · mruby/mruby · GitHub	Issue Tracking Third Party Advisory github.com text/html	MISC github.com/mruby/mruby/issues/4027
[SECURITY] [DLA 2996-1] mruby security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20220506 [SECURITY] [DLA 2996-1] mruby security update

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

179269 Debian Security Update for mruby (DLA 2996-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Mruby	Mruby	1.4.1	All	All	All
Application	Mruby	Mruby	1.4.1	All	All	All

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

cpe:2.3:a:mruby:mruby:1.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:mruby:mruby:1.4.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→