



CVE-2017-9228

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2017-9228
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-24 15:29:00 UTC
Updated	2022-07-20 16:34:00 UTC
Description	An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 5.6.40. The issue is a heap overflow that can be triggered by a crafted input string. The issue is caused by a buffer overflow in the next_state_val() function. The issue is caused by a buffer overflow in the next_state_val() function. The issue is caused by a buffer overflow in the next_state_val() function.

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oniguruma Project	Oniguruma	6.2.0	All	All	All
Application	Oniguruma Project	Oniguruma	6.2.0	All	All	All
Application	Php	Php	All	All	All	All
Application	Php	Php	All	All	All	All
Application	Ruby-lang	Ruby	All	All	All	All

References

Reference	Source	Link
fix #60 : invalid state(CCS_VALUE) in parse_char_class() · kkos/oniguruma@3b63d12 · GitHub	CONFIRM	github.com
Heap corruption in next_state_val() due to uninitialized local variable · Issue #60 · kkos/oniguruma · GitHub	CONFIRM	github.com
Red Hat Customer Portal	REDHAT	access.redhat.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[356443](#) Amazon Linux Security Advisory for oniguruma : ALAS2-2023-2311

[356771](#) Amazon Linux Security Advisory for Hypertext Preprocessor (PHP) : ALAS2-2023-2375

[356983](#) Amazon Linux Security Advisory for oniguruma : AL2012-2023-467

© [CVE.report](#) 2026 |

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](#)