



CVE-2017-9224

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2017-9224
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 16:38:00 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 buffer overflow in the match_at() function. It can be triggered by a crafted string that causes the function to read beyond the end of the input buffer. This can lead to a denial of service or, in some cases, a remote code execution. The issue was discovered by kkos and reported to the vendor. The vendor has released a patch for the issue in version 6.2.1.

Risk And Classification

Problem Types: CWE-125

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 #57 : DATA_ENSURE() check must be before data access · kkos/oniguruma@690313a · GitHub	CONFIRM	github.com
Buffer Overflow in match_at() · Issue #57 · kkos/oniguruma · GitHub	CONFIRM	github.com
Oniguruma Multiple Memory Corruption Vulnerabilities	BID	www.securityfocus.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

355776 Amazon Linux Security Advisory for ruby : ALAS2-2023-2201

355835 Amazon Linux Security Advisory for oniguruma : ALAS2-2023-2217

356990 Amazon Linux Security Advisory for oniguruma : AL2012-2023-474

© [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](#)