



CVE-2017-14064

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

Summary

CVE	CVE-2017-14064
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-31 17:29:00 UTC
Updated	2019-05-13 18:48:00 UTC
Description	Ruby through 2.2.7, 2.3.x through 2.3.4, and 2.4.x through 2.4.1 can expose arbitrary memory during a JSON.generate call

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All

Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Ruby-lang	Ruby	2.3.0	All	All	All
Application	Ruby-lang	Ruby	2.3.0	preview1	All	All
Application	Ruby-lang	Ruby	2.3.0	preview2	All	All
Application	Ruby-lang	Ruby	2.3.1	All	All	All
Application	Ruby-lang	Ruby	2.3.2	All	All	All
Application	Ruby-lang	Ruby	2.3.3	All	All	All
Application	Ruby-lang	Ruby	2.3.4	All	All	All
Application	Ruby-lang	Ruby	2.4.0	All	All	All
Application	Ruby-lang	Ruby	2.4.0	preview1	All	All
Application	Ruby-lang	Ruby	2.4.0	preview2	All	All
Application	Ruby-lang	Ruby	2.4.0	preview3	All	All
Application	Ruby-lang	Ruby	2.4.0	rc1	All	All
Application	Ruby-lang	Ruby	2.4.1	All	All	All
Application	Ruby-lang	Ruby	2.3.0	All	All	All
Application	Ruby-lang	Ruby	2.3.0	preview1	All	All
Application	Ruby-lang	Ruby	2.3.0	preview2	All	All
Application	Ruby-lang	Ruby	2.3.1	All	All	All
Application	Ruby-lang	Ruby	2.3.2	All	All	All
Application	Ruby-lang	Ruby	2.3.3	All	All	All
Application	Ruby-lang	Ruby	2.3.4	All	All	All
Application	Ruby-lang	Ruby	2.4.0	All	All	All
Application	Ruby-lang	Ruby	2.4.0	preview1	All	All

Application	Ruby-lang	Ruby	2.4.0	preview2	All	All
Application	Ruby-lang	Ruby	2.4.0	preview3	All	All
Application	Ruby-lang	Ruby	2.4.0	rc1	All	All
Application	Ruby-lang	Ruby	2.4.1	All	All	All
Application	Ruby-lang	Ruby	All	All	All	All

References

Reference

[Ruby 2.2.8 Released](#)

[Red Hat Customer Portal](#)

[\[SECURITY\] \[DLA 1421-1\] ruby2.1 security update](#)

[Red Hat Customer Portal](#)

[Apple macOS/OS X Multiple Remote Code Execution, Denial of Service, and Information Disclosure Attacks and Local Privilege Escalation At](#)

[Ruby: Multiple vulnerabilities \(GLSA 201710-18\) — Gentoo security](#)

[Fix arbitrary heap exposure problem · flori/json@8f782fd · GitHub](#)

[Ruby Multiple Flaws Let Remote Users Inject Log Data, Deny Service, and Obtain Potentially Sensitive Information from the Heap - SecurityTr](#)

[Bug #13853: Backport request r58323 - Ruby master - Ruby Issue Tracking System](#)

[USN-3685-1: Ruby vulnerabilities | Ubuntu security notices](#)

[HackerOne](#)

[Red Hat Customer Portal](#)

[Red Hat Customer Portal](#)

[Ruby CVE-2017-14064 Arbitrary Memory Disclosure Vulnerability](#)

[Ruby 2.3.5 Released](#)

[Debian -- Security Information -- DSA-3966-1 ruby2.3](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[500608](#) Alpine Linux Security Update for ruby

[504368](#) Alpine Linux Security Update for ruby

[710368](#) Gentoo Linux Ruby Multiple Vulnerabilities (GLSA 201710-18)

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](#)