



CVE-2018-6914

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

Summary

CVE	CVE-2018-6914
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-03 22:29:00 UTC
Updated	2019-07-21 12:15:00 UTC
Description	Directory traversal vulnerability in the Dir.mktmpdir method in the tmpdir library in Ruby before 2.2.10, 2.3.x before 2.3.7, 2.

Risk And Classification

Problem Types: CWE-22

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	7.0	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	Debian	Debian Linux	7.0	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	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.4	All	All	All
Operating System	Redhat	Enterprise Linux	7.5	All	All	All
Operating System	Redhat	Enterprise Linux	7.6	All	All	All

Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.4	All	All	All
Operating System	Redhat	Enterprise Linux	7.5	All	All	All
Operating System	Redhat	Enterprise Linux	7.6	All	All	All
Application	Ruby-lang	Ruby	All	All	All	All
Application	Ruby-lang	Ruby	2.6.0	preview1	All	All
Application	Ruby-lang	Ruby	All	All	All	All
Application	Ruby-lang	Ruby	2.6.0	preview1	All	All

References

Reference

[Red Hat Customer Portal](#)

[Ruby 2.5.1 Released](#)

[Red Hat Customer Portal](#)

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

[Red Hat Customer Portal](#)

[\[SECURITY\] \[DLA 1359-1\] ruby1.8 security update](#)

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

[Red Hat Customer Portal](#)

[CVE-2018-6914: Unintentional file and directory creation with directory traversal in tempfile and tmpdir](#)

[USN-3626-1: Ruby vulnerabilities | Ubuntu security notices](#)

[Ruby 2.4.4 Released](#)

[Ruby 2.2.10 Released](#)

[\[security-announce\] openSUSE-SU-2019:1771-1: important: Security update](#)

[Debian -- Security Information -- DSA-4259-1 ruby2.3](#)

[\[SECURITY\] \[DLA 1358-1\] ruby1.9.1 security update](#)

[Ruby CVE-2018-6914 Directory Traversal Vulnerability](#)

[Ruby 2.3.7 Released](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

377477 Alibaba Cloud Linux Security Update for ruby (ALINUX2-SA-2019:0111)

500610 Alpine Linux Security Update for ruby

504370 Alpine Linux Security Update for ruby

© [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](#)