



CVE-2019-5477

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

Summary

CVE	CVE-2019-5477
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-08-16 16:15:00 UTC
Updated	2022-10-14 18:46:00 UTC
Description	A command injection vulnerability in Nokogiri v1.10.3 and earlier allows commands to be executed in a subprocess via Rub

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Nokogiri	Nokogiri	All	All	All	All

References

Reference	Source	Link
USN-4175-1: Nokogiri vulnerability Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com
CVE-2019-5477 - Nokogiri Command Injection Vulnerability · Issue #1915 · sparklemotion/nokogiri · GitHub	CONFIRM	github.com

[SECURITY] [DLA 3149-1] ruby-nokogiri security update	MLIST	lists.debian.org
HackerOne	MISC	hackerone.com
Nokogiri: Command injection (GLSA 202006-05) — Gentoo security	GENTOO	security.gentoo.org
[SECURITY] [DLA 3150-1] rexical security update	MLIST	lists.debian.org
rexical/CHANGELOG.rdoc at master · tenderlove/rexical · GitHub	MISC	github.com
[SECURITY] [DLA 1933-1] ruby-nokogiri security update	MLIST	lists.debian.org
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

- [181133](#) Debian Security Update for rexical (DLA 3150-1)
- [181134](#) Debian Security Update for ruby-nokogiri (DLA 3149-1)
- [501236](#) Alpine Linux Security Update for ruby-nokogiri
- [505378](#) Alpine Linux Security Update for ruby-nokogiri
- [750375](#) OpenSUSE Security Update for rubygem-nokogiri (openSUSE-SU-2021:0237-1)

© [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