



CVE-2018-12029

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2018-12029
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-17 20:29:00 UTC
Updated	2019-03-08 14:12:00 UTC
Description	A race condition in the nginx module in Phusion Passenger 3.x through 5.x before 5.3.2 allows local escalation of privileges

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Phusion	Passenger	All	All	All	All
Application	Phusion	Passenger	All	All	All	All

References

Reference	Source	Link	Tags
Passenger 5.3.2: various security fixes	MISC	blog.phusion.nl	Mitigation, Vendor Advisory
Phusion Passenger chown() race privilege escalation (CVE-2018-12029)	MISC	pulsesecurity.co.nz	Third Party Advisory
Passenger: Multiple Vulnerabilities (GLSA 201807-02) — Gentoo security	GENTOO	security.gentoo.org	Third Party Advisory
[SECURITY] [DLA 1399-1] ruby-passenger security update	MLIST	lists.debian.org	Mailing List, Third Party Adviso
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)