



CVE-2018-1108

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2018-1108
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-05-21 21:29:00 UTC
Updated	2022-11-29 18:45:00 UTC
Description	kernel drivers before version 4.17-rc1 are vulnerable to a weakness in the Linux kernel's implementation of random seed da

Risk And Classification

Problem Types: CWE-330

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	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link	T
Debian -- Security Information -- DSA-4188-1 linux	DEBIAN	www.debian.org	T
USN-3752-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	T
USN-3752-2: Linux kernel (HWE) vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	T
Bug 1567306 – CVE-2018-1108 kernel: drivers: getrandom(2) unblocks too early after system boot	CONFIRM	bugzilla.redhat.com	Is
Linux Kernel CVE-2018-1108 Predictable Random Number Generator Weakness	BID	www.securityfocus.com	T
[SECURITY] [DLA 3065-1] linux security update	MLIST	lists.debian.org	
USN-3752-3: Linux kernel (Azure, GCP, OEM) vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	T
USN-3718-1: Linux kernel regression Ubuntu security notices	UBUNTU	usn.ubuntu.com	T

USN-3718-2: Linux kernel (HWE) regression Ubuntu security notices	UBUNTU	usn.ubuntu.com	T
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[180282](#) Debian Security Update for linux (DLA 3065-1)

© [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