



CVE-2018-1126

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

Summary

CVE	CVE-2018-1126
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-05-23 13:29:00 UTC
Updated	2019-07-30 13:15:00 UTC
Description	procps-ng before version 3.3.15 is vulnerable to an incorrect integer size in proc/alloc.* leading to truncation/integer overflow

Risk And Classification

Problem Types: CWE-190

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	18.04	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	Canonical	Ubuntu Linux	18.04	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
Application	Procps-ng Project	Procps-ng	All	All	All	All
Application	Procps-ng Project	Procps-ng	All	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All

Operating System	Redhat	Enterprise Linux	7.0	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	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.6	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	Schneider-electric	Struxeware Data Center Expert	All	All	All	All
Application	Schneider-electric	Struxeware Data Center Expert	All	All	All	All

References

Reference	Source
[security-announce] openSUSE-SU-2019:2376-1: important: Security update	SUSE
Red Hat Customer Portal	REDH
www.qualys.com/2018/05/17/procps-ng-audit-report-advisory.txt	MISC
Debian -- Security Information -- DSA-4208-1 procps	DEBI
Bug 1575853 – CVE-2018-1126 procps-ng, procps: incorrect integer size in proc/alloc.* leading to truncation / integer overflow issues	CONF
Red Hat Customer Portal	REDH
Procps-ng Procps Multiple Security Vulnerabilities	BID
[SECURITY] [DLA 1390-1] procps security update	MLIS
Red Hat Customer Portal	REDH
DCIM Support	CONF
oss-sec: Qualys Security Advisory - Procps-ng Audit Report	MLIS
USN-3658-1: procps-ng vulnerabilities Ubuntu security notices Ubuntu	UBUN
Red Hat Customer Portal	REDH
USN-3658-2: procps-ng vulnerabilities Ubuntu security notices	UBUN
Red Hat Enterprise Virtualization Integer Overflows in procps-ng Lets Local Users Gain Elevated Privileges - SecurityTracker	SECT
Red Hat Customer Portal	REDH
Red Hat Customer Portal	REDH

[security-announce] opensUSE-SU-2019:2379-1: important: Security update	SUSE
CVE Program record	CVE
NVD vulnerability detail	NVD
<div style="border: 1px solid #ccc; height: 15px; background-color: #f0f0f0; margin-bottom: 5px;"></div> <div style="background-color: #e0f2f7; padding: 5px; text-align: center;">No vendor comments have been submitted for this CVE.</div>	
Legacy QID Mappings	
296077 Oracle Solaris 11.4 Support Repository Update (SRU) 18.4.0 Missing (CPUJAN2020)	

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://cve.mitre.org). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report