



# CVE-2018-1123

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary


<b>CVE</b>	CVE-2018-1123
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-05-23 14:29:00 UTC
<b>Updated</b>	2023-11-07 02:55:00 UTC
<b>Description</b>	procps-ng before version 3.3.15 is vulnerable to a denial of service in ps via mmap buffer overflow. Inbuilt protection in ps n

## Risk And Classification

**Problem Types:** CWE-122

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	17.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	17.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Procps-ng Project</a>	<a href="#">Procps-ng</a>	All	All	All	All

Application	Procps-ng Project	Procps-ng	All	All	All	All
<b>References</b>						
<b>Reference</b>						
[security-announce] openSUSE-SU-2019:2376-1: important: Security update						
www.qualys.com/2018/05/17/procps-ng-audit-report-advisory.txt						
Debian -- Security Information -- DSA-4208-1 procps						
Procps-ng Procps Multiple Security Vulnerabilities						
[bookkeeper-issues] 20210628 [GitHub] [bookkeeper] padma81 opened a new issue #2746: Security Vulnerabilities in CentOS 7 image, Upgrade						
[SECURITY] [DLA 1390-1] procps security update						
Pony Mail!						
USN-3658-3: procps-ng vulnerabilities   Ubuntu security notices						
oss-sec: Qualys Security Advisory - Procps-ng Audit Report						
Procps-ng - Multiple Vulnerabilities - Linux local Exploit						
USN-3658-1: procps-ng vulnerabilities   Ubuntu security notices   Ubuntu						
procps: Multiple vulnerabilities (GLSA 201805-14) — Gentoo security						
Bug 1575474 – CVE-2018-1123 procps-ng, procps: denial of service in ps via mmap buffer overflow						
Pony Mail!						
[bookkeeper-issues] 20210629 [GitHub] [bookkeeper] padma81 opened a new issue #2746: Security Vulnerabilities in CentOS 7 image, Upgrade						
[security-announce] openSUSE-SU-2019:2379-1: important: Security update						
CVE Program record						
NVD vulnerability detail						
						
No vendor comments have been submitted for this CVE.						
There are currently no legacy QID mappings associated with this CVE.						

© 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](#)**