



# CVE-2018-1125

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

## Summary

<b>CVE</b>	CVE-2018-1125
<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>	2020-09-09 14:59:00 UTC
<b>Description</b>	procps-ng before version 3.3.15 is vulnerable to a stack buffer overflow in pgrep. This vulnerability is mitigated by FORTIFY

## Risk And Classification

**Problem Types:** CWE-787

## 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
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All

Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Application	<a href="#">Procps-ng Project</a>	<a href="#">Procps-ng</a>	All	All	All	All
Application	<a href="#">Procps-ng Project</a>	<a href="#">Procps-ng</a>	All	All	All	All

## References

Reference	Source	Link	Tags
[security-announce] openSUSE-SU-2019:2376-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List, Third
<a href="http://www.qualys.com/2018/05/17/procps-ng-audit-report-advisory.txt">www.qualys.com/2018/05/17/procps-ng-audit-report-advisory.txt</a>	MISC	<a href="http://www.qualys.com">www.qualys.com</a>	Exploit, Third Part
Debian -- Security Information -- DSA-4208-1 procps	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	Third Party Advise
Procps-ng Procps Multiple Security Vulnerabilities	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Third Party Advise
[SECURITY] [DLA 1390-1] procps security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	Mailing List, Third
USN-3658-3: procps-ng vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	Third Party Advise
Bug 1575852 – CVE-2018-1125 procps-ng, procps: stack buffer overflow in pgrep	CONFIRM	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	Issue Tracking
oss-sec: Qualys Security Advisory - Procps-ng Audit Report	MLIST	<a href="https://seclists.org">seclists.org</a>	Mailing List, Third
USN-3658-1: procps-ng vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	Third Party Advise
[security-announce] openSUSE-SU-2019:2379-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List, Third
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysi

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](https://status.cve.report)