CVE-2018-1122

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-1122
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-05-23 14:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	procps-ng before version 3.3.15 is vulnerable to a local privilege escalation in top. If a user runs top with HOME unset in an

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	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	Canonical	Ubuntu Linux	12.04	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

References

Reference	Source	Link	Tags
[security-announce] openSUSE-SU-2019:2376-1: important: Security update	SUSE	lists.opensuse.org	
www.qualys.com/2018/05/17/procps-ng-audit-report-advisory.txt	MISC	www.qualys.com	Exploit, Third
Bug 1575466 – CVE-2018-1122 procps-ng, procps: Local privilege escalation in top	CONFIRM	bugzilla.redhat.com	Issue Trackin
Debian -- Security Information -- DSA-4208-1 procps	DEBIAN	www.debian.org	Third Party A
Procps-ng Procps Multiple Security Vulnerabilities	BID	www.securityfocus.com	Third Party A
[SECURITY] [DLA 1390-1] procps security update	MLIST	lists.debian.org	Third Party A
USN-3658-3: procps-ng vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third Party A
Red Hat Customer Portal	REDHAT	access.redhat.com	
oss-sec: Qualys Security Advisory - Procps-ng Audit Report	MLIST	seclists.org	Mailing List, T
Procps-ng - Multiple Vulnerabilities - Linux local Exploit	EXPLOIT-DB	www.exploit-db.com	Exploit, Third
USN-3658-1: procps-ng vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	Third Party A
procps: Multiple vulnerabilities (GLSA 201805-14) — Gentoo security	GENTOO	security.gentoo.org	Third Party A
Red Hat Customer Portal	REDHAT	access.redhat.com	
[security-announce] openSUSE-SU-2019:2379-1: important: Security update	SUSE	lists.opensuse.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

296077 Oracle Solaris 11.4 Support Repository Update (SRU) 18.4.0 Missing (CPUJAN2020)

375932 F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) procps-ng Vulnerability (K00409335)

377279 Alibaba Cloud Linux Security Update for procps-ng (ALINUX2-SA-2019:0089)