



CVE-2018-1121

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2018-1121
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-13 20:29:00 UTC
Updated	2020-06-30 16:15:00 UTC
Description	procps-ng, procps is vulnerable to a process hiding through race condition. Since the kernel's proc_pid_readdir() returns PII

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Procps Project	Procps	All	All	All	All

References

Reference	Source	Link
www.qualys.com/2018/05/17/procps-ng-audit-report-advisory.txt	MISC	www.qualys.com
Procps-ng Procps Multiple Security Vulnerabilities	BID	www.securityfocus.com
oss-sec: Qualys Security Advisory - Procps-ng Audit Report	MLIST	seclists.org
Bug 1575473 – CVE-2018-1121 procps-ng, procps: process hiding through race condition enumerating /proc	CONFIRM	bugzilla.redhat.com
Procps-ng - Multiple Vulnerabilities - Linux local Exploit	EXPLOIT-DB	www.exploit-db.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)