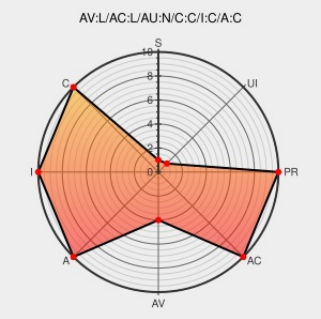
CVE-2013-7135

Published on: 01/27/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:34 PM UTC

CVE-2013-7135

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Proc from Detlef Pilzecker contain the following vulnerability:

The Proc::Daemon module 0.14 for Perl uses world-writable permissions for a file that stores a process ID, which allows local users to have an unspecified impact by modifying this file.

CVE-2013-7135 has been assigned by security@debian.org to track the vulnerability

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
oss-security - Bug#732283: CVE Request: Proc::Daemon writes pidfile with mode 666	www.openwall.com text/html	MLIST [oss-security] 20131217 Bug#732283: CVE Request: Proc::Daemon writes pidfile with mode 666
oss-security - CVE Request: Proc::Daemon writes pidfile with mode 666	www.openwall.com text/html	MLIST [oss-security] 20131216 CVE Request: Proc::Daemon writes pidfile with mode 666
oss-security - Re: CVE Request: Proc::Daemon writes pidfile with mode 666	www.openwall.com text/html	MLIST [oss-security] 20131217 Re: CVE Request: Proc::Daemon writes pidfile with mode 666
Bug #91450 for Proc-Daemon: Fwd: Bug#732283: libproc-daemon-perl: Writes pidfile with mode 666	rt.cpan.org text/html	MISC rt.cpan.org/Public/Bug/Display.html?id=91450
Support / Security / Advisories / / MDVSA-2014:021 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2014:021

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Detlef Pilzecker	Proc		adaemon-run_perl	0.14	All
Application	Detlef Pilzecker	Proc	\	adaemon-run_perl	0.14	All
Application	Detlef Pilzecker	Proc	\	adaemon-run_perl	0.14	All

cpe:2.3:a:detlef_pilzecker:proc::adaemon-run_perl:0.14:*:*:*:*:*:*:

cpe:2.3:a:detlef_pilzecker:proc\:\:adaemon-run_perl:0.14:*:*:*:*:*:*:

cpe:2.3:a:detlef_pilzecker:proc\:\:adaemon-run_perl:0.14:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | |
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 registred 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