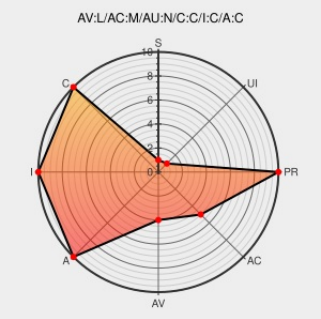
CVE-2011-4122

Published on: 11/17/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:12 PM UTC

CVE-2011-4122

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



Certain versions of Freebsd from Freebsd contain the following vulnerability:

Directory traversal vulnerability in openpam_configure.c in OpenPAM before r478 on FreeBSD 8.1 allows local users to load arbitrary DSOs and gain privileges via a .. (dot dot) in the service_name argument to the pam_start function, as demonstrated by a .. in the -c option to kcheckpass.

CVE-2011-4122 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.9 - MEDIUM

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

CVE References

Description	Tags	Link
Changeset 478 for trunk/lib/openpam_configure.c – OpenPAM	trac.des.no text/html	CONFIRM trac.des.no/openpam/changeset/478/trunk/lib/openpam_configure.c
Security Advisory SA46804 - FreeBSD OpenPAM Privilege Escalation Security Issue - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 46804
oss-security - Disputing CVE-2011-4122	openwall.com text/html	MLIST [oss-security] 20111207 Disputing CVE-2011-4122
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 76945

C-skills: openpam trickery	Exploit c-skills.blogspot.com text/html	MISC c-skills.blogspot.com/2011/11/openpam-trickery.html
oss-security - Re: Disputing CVE-2011-4122	openwall.com text/html	MLIST [oss-security] 20111208 Re: Disputing CVE-2011-4122
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF openpam-Pamstart-privilege-escalation(71205)
	stealth.openwall.net text/x-perl	MISC stealth.openwall.net/xSports/pamslam
About Secunia Research | Flexera	Vendor Advisory secunia.com Depreciated Link text/plain	SECUNIA 46756

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
Operating System	Freebsd	Freebsd	8.1	All	All	All
Operating System	Freebsd	Freebsd	8.1	All	All	All

cpe:2.3:o:freebsd:freebsd:8.1:*:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:8.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→