CVE-2017-12197

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-12197
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-18 21:29:00 UTC
Updated	2019-10-09 23:22:00 UTC
Description	It was found that libpam4j up to and including 1.8 did not properly validate user accounts when authenticating. A user with a

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	Libpam4j Project	Libpam4j	All	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All

References

Reference	Source	Link	Tags
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Party Advisory
1503103 – (CVE-2017-12197) CVE-2017-12197 libpam4j: Account check bypass	CONFIRM	bugzilla.redhat.com	Issue Tracking, Third P
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Party Advisory
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Party Advisory
[SECURITY] [DLA 1165-1] libpam4j security update	MLIST	lists.debian.org	Third Party Advisory

Debian -- Security Information -- DSA-4025-1 libpam4j	DEBIAN	www.debian.org	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.