CVE-2016-6866

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

Summary

CVE	CVE-2016-6866
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-15 19:59:00 UTC
Updated	2023-11-07 02:34:00 UTC
Description	slock allows attackers to bypass the screen lock via vectors involving an invalid password hash, which triggers a NULL poin

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	24	All	All	All
Operating System	Fedoraproject	Fedora	25	All	All	All
Operating System	Fedoraproject	Fedora	24	All	All	All
Operating System	Fedoraproject	Fedora	25	All	All	All
Application	Suckless	Slock	All	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] Fedora 24 Update: slock-1.3-2.fc24 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Third P
fix CVE-2016-6866 - slock - simple X display locker utility	CONFIRM	git.suckless.org	Patch,
oss-security - Re: CVE request - slock, all versions NULL pointer dereference	MLIST	www.openwall.com	Mailing
oss-security - CVE request - slock, all versions NULL pointer dereference	MLIST	www.openwall.com	Mailing
s1m0n.dft-labs.eu/files/slock/slock.txt	MISC	s1m0n.dft-labs.eu	Third P
[SECURITY] Fedora 24 Update: slock-1.3-2.fc24 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
slock CVE-2016-6866 NULL Pointer Dereference Denial of Service Vulnerability	BID	www.securityfocus.com	Third P
[SECURITY] Fedora 25 Update: slock-1.3-2.fc25 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 25 Update: slock-1.3-2.fc25 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Third P

CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

501372 Alpine Linux Security Update for slock

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**