CVE-2010-0393

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

Summary

CVE	CVE-2010-0393
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-03-05 19:30:00 UTC
Updated	2013-05-15 03:06:00 UTC
Description	The _cupsGetlang function, as used by lppasswd.c in lppasswd in CUPS 1.2.2, 1.3.7, 1.3.9, and 1.4.1, relies on an environ

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apple	Cups	1.2.2	All	All	All
Application	Apple	Cups	1.3.7	All	All	All
Application	Apple	Cups	1.3.9	All	All	All
Application	Apple	Cups	1.4.1	All	All	All
Application	Apple	Cups	1.2.2	All	All	All
Application	Apple	Cups	1.3.7	All	All	All
Application	Apple	Cups	1.3.9	All	All	All
Application	Apple	Cups	1.4.1	All	All	All

References

Reference	Source	Link
Setuid programs should not be allowed to override default dirs · Issue #3482 · apple/cups · GitHub	MISC	www.cups.org
USN-906-1: CUPS vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.com
APPLE-SA-2010-03-29-1 Security Update 2010-002 / Mac OS X v10.6.3	APPLE	lists.apple.com
Bug 558460 – CVE-2010-0393: cups possible arbitrary code execution via suid lppasswd (STR #3482)	CONFIRM	bugzilla.redhat.com
Gentoo Linux Documentation -- CUPS: Multiple vulnerabilities	GENTOO	security.gentoo.org
Support / Security / Advisories / / MDVSA-2010:072 | Mandriva	MANDRIVA	www.mandriva.com

CUPS 'lppasswd' Tool Localized Message String Security Weakness	BID	www.securityfocus.co
Support / Security / Advisories / / MDVSA-2010:073 | Mandriva	MANDRIVA	www.mandriva.com
About the security content of Security Update 2010-002 / Mac OS X v10.6.3	CONFIRM	support.apple.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2010-03-09	Tomas Hoger	This issue did not affected Red Hat Enterprise Linux 3 and 4 due to the lack of localization in lp

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