CVE-2006-3126

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

Summary

CVE	CVE-2006-3126
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-09-06 00:04:00 UTC
Updated	2011-03-08 02:37:00 UTC
Description	c2faxrecv in capi4hylafax 01.02.03 allows remote attackers to execute arbitrary commands via null (\0) and shell metachara

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Julian Pawlowski	Capi4hylafax	01.02.03	All	All	All
Application	Julian Pawlowski	Capi4hylafax	01.02.03	All	All	All

References

Reference	Source	Link
Capi4Hylafax Shell Command Injection - Advisories - Secunia	SECUNIA	secunia.com
Gentoo Linux Documentation -- CAPI4Hylafax fax receiver: Execution of arbitrary code	GENTOO	security.gentoo.org
Debian update for capi4hylafax - Advisories - Secunia	SECUNIA	secunia.com
#382474 - capi4hylafax: c2faxrecv problem with anonymous incoming calls - Debian Bug report logs	MISC	bugs.debian.org
Gentoo update for capi4hylafax - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
Security Announcement	SUSE	www.novell.com
Debian -- Security Information -- DSA-1165-1 capi4hylafax	DEBIAN	www.debian.org
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
CAPI4Hylafax Remote Arbitrary Command Execution Vulnerability	BID	www.securityfocus.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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