CVE-2005-3539

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

Summary

CVE	CVE-2005-3539
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-12-31 05:00:00 UTC
Updated	2018-10-19 15:36:00 UTC
Description	Multiple eval injection vulnerabilities in HylaFAX 4.2.3 and earlier allow remote attackers to execute arbitrary commands via

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hylafax	Hylafax	4.1.1	All	All	All
Application	Hylafax	Hylafax	4.2	All	All	All
Application	Hylafax	Hylafax	4.2.1	All	All	All
Application	Hylafax	Hylafax	4.2.2	All	All	All
Application	Hylafax	Hylafax	4.2.3	All	All	All
Application	Hylafax	Hylafax	4.1.1	All	All	All
Application	Hylafax	Hylafax	4.2	All	All	All
Application	Hylafax	Hylafax	4.2.1	All	All	All
Application	Hylafax	Hylafax	4.2.2	All	All	All
Application	Hylafax	Hylafax	4.2.3	All	All	All

References

Reference	Source	Link	Tag
Secunia - Advisories - Mandriva update for hylafax	SECUNIA	secunia.com	
Debian -- Page not found	DEBIAN	www.debian.org	
Bug 719 - Unsanitised user-supplied data passed to eval in notify and faxrcvd	MISC	bugs.hylafax.org	
HylaFAX 4.2.4 release - hylafax.org	CONFIRM	www.hylafax.org	

Secunia - Advisories - HylaFAX Authentication Bypass and Command Insertion Vulnerabilities	SECUNIA	secunia.com	Patc
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	
Gentoo Linux Documentation -- HylaFAX: Multiple vulnerabilities	GENTOO	www.gentoo.org	Patc
Secunia - Advisories - Gentoo update for hylafax	SECUNIA	secunia.com	Patc
SecurityFocus	BUGTRAQ	www.securityfocus.com	
Hylafax Multiple Scripts Remote Command Execution Vulnerability	BID	www.securityfocus.com	Exp
Secunia - Advisories - Debian update for hylafax	SECUNIA	secunia.com	
Advisories - Mandriva Linux	MANDRIVA	www.mandriva.com	
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

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**