CVE-2005-3347

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

Summary

CVE	CVE-2005-3347
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-11-18 02:02:00 UTC
Updated	2017-07-11 01:33:00 UTC
Description	Multiple directory traversal vulnerabilities in index.php in phpSysInfo 2.4 and earlier, as used in phpgroupware 0.9.16 and e

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Phpgroupware	Phpgroupware	0.9.16	All	All	All
Application	Phpgroupware	Phpgroupware	0.9.16	All	All	All

References

Reference	Source	Link
Debian -- Security Information -- DSA-897-1 phpsysinfo	DEBIAN	www.debian.org
Secunia - Advisories - Debian update for phpsysinfo	SECUNIA	secunia.com
Advisories - Mandriva Linux	MANDRIVA	www.mandriva.com
Secunia - Advisories - phpSysInfo "register_globals" Emulation Layer Overwrite Vulnerability	SECUNIA	secunia.com
Hardened-PHP Project - PHP Security - Advisory 22/2005	MISC	www.hardened-php.net
Debian -- Security Information -- DSA-899-1 egroupware	DEBIAN	www.debian.org
PHPSysInfo Multiple Input Validation Vulnerabilities	BID	www.securityfocus.com
Gentoo Linux Documentation -- phpSysInfo: Multiple vulnerabilities	GENTOO	www.gentoo.org
Secunia - Advisories - phpGroupWare Multiple Vulnerabilities	SECUNIA	secunia.com
Secunia - Advisories - eGroupWare Multiple Vulnerabilities	SECUNIA	secunia.com
Debian -- Security Information -- DSA-898-1 phpgroupware	DEBIAN	www.debian.org
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com

SecurityFocus	BUGTRAQ	www.securityfocus.com
Secunia - Advisories - Debian update for phpgroupware	SECUNIA	secunia.com
PHPsysInfo Multiple Input Validation Vulnerabilities	BID	www.securityfocus.com
Secunia - Advisories - Debian update for egroupware	SECUNIA	secunia.com
Secunia - Advisories - Gentoo update for phpsysinfo	SECUNIA	secunia.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**