CVE-2006-0097

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

Summary

CVE	CVE-2006-0097
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-01-06 11:03:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Stack-based buffer overflow in the create_named_pipe function in libmysql.c in PHP 4.3.10 and 4.4.x before 4.4.3 for Windo

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:P

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Php	Php	4.3.10	All	All	All

Application	Php	Php	4.4.0	All	All	All
Application	Php	Php	4.4.1	All	All	All
Application	Php	Php	4.4.2	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
[Full-disclosure] Windows PHP 4.x "0-day" buffer overflow	af854a3a-2127-422b-91a
PHP "mysql_connect" Buffer Overflow Vulnerability - Advisories - Secunia	af854a3a-2127-422b-91a
Webmail - OVH	af854a3a-2127-422b-91a
PHP: PHP 4 ChangeLog	af854a3a-2127-422b-91a
PHP MySQL_Connect Remote Buffer Overflow Vulnerability	af854a3a-2127-422b-91a
www.osvdb.org/22232	af854a3a-2127-422b-91a
Neohapsis Archives - Full Disclosure List - #0274 - [Full-disclosure] RE: Windows PHP 4.x "0-day" buffer overflow	af854a3a-2127-422b-91a
SecurityFocus	af854a3a-2127-422b-91a
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2008-10-30	Tomas Hoger	Not vulnerable. This issue did not affect the versions of php as shipped with Red Hat Enterprise

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