CVE-2006-6966

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

Summary

CVE	CVE-2006-6966
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-02-04 00:28:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	phpGraphy before 0.9.13a does not properly unset variables when the input data includes a numeric parameter with a value

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: NVD-CWE-Other | 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	Phpgraphy	Phpgraphy	0.9	All	All	All

Application	Phpgraphy	Phpgraphy	0.9.1	All	All	All
Application	Phpgraphy	Phpgraphy	0.9.10	All	All	All
Application	Phpgraphy	Phpgraphy	0.9.10a	All	All	All
Application	Phpgraphy	Phpgraphy	0.9.11	All	All	All
Application	Phpgraphy	Phpgraphy	0.9.12	All	All	All
Application	Phpgraphy	Phpgraphy	0.9.2	All	All	All
Application	Phpgraphy	Phpgraphy	0.9.3	All	All	All
Application	Phpgraphy	Phpgraphy	0.9.4	All	All	All
Application	Phpgraphy	Phpgraphy	0.9.5	All	All	All
Application	Phpgraphy	Phpgraphy	0.9.6	All	All	All
Application	Phpgraphy	Phpgraphy	0.9.7	All	All	All
Application	Phpgraphy	Phpgraphy	0.9.8	All	All	All
Application	Phpgraphy	Phpgraphy	0.9.9	All	All	All
Application	Phpgraphy	Phpgraphy	0.9.9a	All	All	All
Application	Phpgraphy	Phpgraphy	All	All	All	All

Vendor Declared Affected Products

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

References

Reference
phpGraphy - Changelog - Official Site
Error 404 :(
SourceForge.net: News: 0.9.13a security fix release
SecurityTracker.com Archives - phpGraphy Zend_Hash_Del_Key_Or_Index Underlying PHP Bug Lets Remote Users Execute Arbitrary Code
IBM X-Force Exchange
CVE Program record
NVD vulnerability detail

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