CVE-2014-4907

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

Summary

CVE	CVE-2014-4907
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-07-11 11:08:22 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cross-site scripting (XSS) vulnerability in share/pnp/application/views/kohana_error_page.php in PNP4Nagios before 0.6.2

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

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

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Op5	Monitor	6.3.0	All	All	All

Application	Pnp4nagios	Pnp4nagios	0.6.0	All	All	All
Application	Pnp4nagios	Pnp4nagios	0.6.1	All	All	All
Application	Pnp4nagios	Pnp4nagios	0.6.10	All	All	All
Application	Pnp4nagios	Pnp4nagios	0.6.11	All	All	All
Application	Pnp4nagios	Pnp4nagios	0.6.12	All	All	All
Application	Pnp4nagios	Pnp4nagios	0.6.13	All	All	All
Application	Pnp4nagios	Pnp4nagios	0.6.14	All	All	All
Application	Pnp4nagios	Pnp4nagios	0.6.15	All	All	All
Application	Pnp4nagios	Pnp4nagios	0.6.16	All	All	All
Application	Pnp4nagios	Pnp4nagios	0.6.17	All	All	All
Application	Pnp4nagios	Pnp4nagios	0.6.18	All	All	All
Application	Pnp4nagios	Pnp4nagios	0.6.19	All	All	All
Application	Pnp4nagios	Pnp4nagios	0.6.2	All	All	All
Application	Pnp4nagios	Pnp4nagios	0.6.20	All	All	All
Application	Pnp4nagios	Pnp4nagios	0.6.3	All	All	All
Application	Pnp4nagios	Pnp4nagios	0.6.4	All	All	All
Application	Pnp4nagios	Pnp4nagios	0.6.5	All	All	All
Application	Pnp4nagios	Pnp4nagios	0.6.6	All	All	All
Application	Pnp4nagios	Pnp4nagios	0.6.7	All	All	All
Application	Pnp4nagios	Pnp4nagios	All	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
oss-security - Re: CVE request: XSS in PNP4Nagios	af854a3a-2127-422b-91ae-364da26611(
Malformed Request	af854a3a-2127-422b-91ae-364da26611(
op5 Monitor 6.3.1 release notes - op5	af854a3a-2127-422b-91ae-364da26611(
pnp-0.6:dwnld [PNP4Nagios Docs]	af854a3a-2127-422b-91ae-364da26611(
0008761: XSS in pnp - op5 bug and feature tracker	af854a3a-2127-422b-91ae-364da26611(
Security Advisory SA59535 - op5 Monitor URL Cross-Site Scripting Vulnerability - Secunia	af854a3a-2127-422b-91ae-364da26611(
PNP4Nagios / Code / Commit [f846a6]	af854a3a-2127-422b-91ae-364da26611(
Security Advisory SA59603 - PNP4Nagios Error Page Cross-Site Scripting Vulnerability - Secunia	af854a3a-2127-422b-91ae-364da26611(
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

NVD vulnerability detail NVD

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**