



CVE-2013-5350

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2013-5350
State	PUBLIC
Assigner	PSIRT-CNA@flexerasoftware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-24 15:08:00 UTC
Updated	2014-01-24 22:00:00 UTC
Description	The "Remember me" feature in the opSecurityUser::getRememberLoginCookie function in lib/user/opSecurityUser.class.ph

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tejimaya	Openpne	3.6.13	All	All	All
Application	Tejimaya	Openpne	3.8.9	All	All	All
Application	Tejimaya	Openpne	3.6.13	All	All	All
Application	Tejimaya	Openpne	3.8.9	All	All	All

References

Reference
【緊急リリース】OpenPNE 3.6.13, 3.8.9 以下の「次回から自動ログイン」機能に存在する PHP Object Injection 脆弱性対応のお知らせ (OP)
About Secunia Research Flexera
JVN#69986880: OpenPNE vulnerable to PHP Object Injection
JVNDB-2014-000009
Security Advisory SA54043 - OpenPNE PHP Object Injection Vulnerability - Secunia
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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)