CVE-2015-2126

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

Summary

CVE	CVE-2015-2126
State	PUBLIC
Assigner	hp-security-alert@hp.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-07-06 14:59:00 UTC
Updated	2016-12-28 02:59:00 UTC
Description	Unspecified vulnerability in pppoec in HP HP-UX 11iv2 and 11iv3 allows local users to gain privileges by leveraging setuid p

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Hp	Hp-ux	11.11iv2	All	All	All
Operating System	Hp	Hp-ux	11.11iv3	All	All	All
Operating System	Hp	Hp-ux	11.11iv2	All	All	All
Operating System	Hp	Hp-ux	11.11iv3	All	All	All

References

Reference	Source	Link
HP-UX 'pppoec' Access Permission Flaw Lets Local Users Gain Root Privileges - SecurityTracker	SECTRACK	www.securitytracker.com
HP-UX CVE-2015-2126 Local Privilege Escalation Vulnerability	BID	www.securityfocus.com
Software and Drivers	HP	h20564.www2.hp.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.

© 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 registred 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