



CVE-2012-0125

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

Summary

CVE	CVE-2012-0125
State	PUBLIC
Assigner	hp-security-alert@hp.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-03-28 10:54:00 UTC
Updated	2017-12-06 02:29:00 UTC
Description	Unspecified vulnerability in the WBEM implementation in HP HP-UX 11.31 allows local users to obtain access to diagnostic

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Hp	Hp-ux	11.31	All	All	All
Operating System	Hp	Hp-ux	11.31	All	All	All

References

Reference	Source	Link
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
HP Technical Support, Help, and Troubleshooting HP® Customer Support	HP	h20566.www2.hp.com
Security Advisory SA48593 - HP-UX WBEM Diagnostic Data Security Bypass Vulnerability - Secunia	SECUNIA	secunia.com
HP WBEM Discloses Diagnostic Data to Remote and Local Users - SecurityTracker	SECTrack	www.securitytracker.com
HP-UX WBEM CVE-2012-0125 Local Unauthorized Access Vulnerability	BID	www.securityfocus.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 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](#)