



CVE-2010-0447

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

Summary

CVE	CVE-2010-0447
State	PUBLIC
Assigner	hp-security-alert@hp.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-03-10 22:30:00 UTC
Updated	2018-10-10 19:52:00 UTC
Description	The helpmanager servlet in the web server in HP OpenView Performance Insight (OVPI) 5.4 and earlier does not properly a

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hp	Openview Performance Insight	All	All	All	All

References

Reference	Source	Link
HP Performance Insight Arbitrary Command Execution Vulnerability - Secunia.com	SECUNIA	secunia.com
'[security bulletin] HPSBMA02489 SSRT090065 rev.1 - HP Performance Insight , Remote Execution of Arbi' - MARC	HP	marc.info
IBM X-Force Exchange	XF	exchange
Zero Day Initiative	MISC	www.zer
SecurityFocus	BUGTRAQ	www.sec
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vup
62797	OSVDB	osvdb.org
HP Performance Insight Remote Command Execution Vulnerability	BID	www.sec
CVE Program record	CVE.ORG	www.cve
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](#)