



CVE-2012-3267

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

Summary

CVE	CVE-2012-3267
State	PUBLIC
Assigner	hp-security-alert@hp.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-10-04 11:11:00 UTC
Updated	2017-08-29 01:31:00 UTC
Description	Unspecified vulnerability in HP Network Node Manager i (NNMi) 9.20 allows remote attackers to obtain sensitive information

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hp	Network Node Manager I	9.20	All	All	All
Application	Hp	Network Node Manager I	9.20	All	All	All

References

Reference	Source	Link
HP Network Node Manager i CVE-2012-3267 Unspecified Information Disclosure Vulnerability	BID	www.sec
HP Technical Support, Help, and Troubleshooting HP® Customer Support	HP	h20565.v
HP Network Node Manager i Discloses Potentially Sensitive Information to Remote Users - SecurityTracker	SECTrack	www.sec
85891	OSVDB	osvdb.or
Security Advisory SA50861 - HP Network Node Manager i Unspecified Information Disclosure Weakness - Secunia	SECUNIA	secunia.c
IBM X-Force Exchange	XF	exchange
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

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](#)