



CVE-2008-1842

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

Summary

CVE	CVE-2008-1842
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-04-16 17:05:00 UTC
Updated	2018-10-11 20:37:00 UTC
Description	Integer signedness error in ovspmd.exe in HP OpenView Network Node Manager (OV NNM) 8.01, and 7.53 and earlier, all

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hp	Openview Network Node Manager	4.11	All	All	All
Application	Hp	Openview Network Node Manager	5.0.1	All	All	All
Application	Hp	Openview Network Node Manager	5.01	All	All	All
Application	Hp	Openview Network Node Manager	6.0.1	All	All	All
Application	Hp	Openview Network Node Manager	6.1	All	All	All
Application	Hp	Openview Network Node Manager	6.10	All	All	All
Application	Hp	Openview Network Node Manager	6.2	All	All	All
Application	Hp	Openview Network Node Manager	6.20	All	All	All
Application	Hp	Openview Network Node Manager	6.31	All	All	All
Application	Hp	Openview Network Node Manager	6.4	All	All	All
Application	Hp	Openview Network Node Manager	6.41	All	All	All
Application	Hp	Openview Network Node Manager	7.0.1	All	All	All
Application	Hp	Openview Network Node Manager	7.01	All	All	All
Application	Hp	Openview Network Node Manager	7.50	All	All	All
Application	Hp	Openview Network Node Manager	7.51	All	All	All
Application	Hp	Openview Network Node Manager	8.01	All	All	All
Application	Hp	Openview Network Node Manager	4.11	All	All	All

Application	Hp	Openview Network Node Manager	5.0.1	All	All	All
Application	Hp	Openview Network Node Manager	5.01	All	All	All
Application	Hp	Openview Network Node Manager	6.0.1	All	All	All
Application	Hp	Openview Network Node Manager	6.1	All	All	All
Application	Hp	Openview Network Node Manager	6.10	All	All	All
Application	Hp	Openview Network Node Manager	6.2	All	All	All
Application	Hp	Openview Network Node Manager	6.20	All	All	All
Application	Hp	Openview Network Node Manager	6.31	All	All	All
Application	Hp	Openview Network Node Manager	6.4	All	All	All
Application	Hp	Openview Network Node Manager	6.41	All	All	All
Application	Hp	Openview Network Node Manager	7.0.1	All	All	All
Application	Hp	Openview Network Node Manager	7.01	All	All	All
Application	Hp	Openview Network Node Manager	7.50	All	All	All
Application	Hp	Openview Network Node Manager	7.51	All	All	All
Application	Hp	Openview Network Node Manager	8.01	All	All	All
Application	Hp	Openview Network Node Manager	All	All	All	All

References

Reference
SecurityTracker.com Archives - HP OpenView Network Node Manager Buffer Overflow in ovspmd Lets Remote Users Execute Arbitrary Code
HP OpenView Network Node Manager ovspmd.exe Buffer Overflow - Advisories - Secunia
SSRT080024
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Luigi Auriemma
alugi.altervista.org/adv/closedview-adv.txt
SecurityFocus
HP OpenView Network Node Manager 'ovspmd' Buffer Overflow Vulnerability
IBM X-Force Exchange
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](#)