

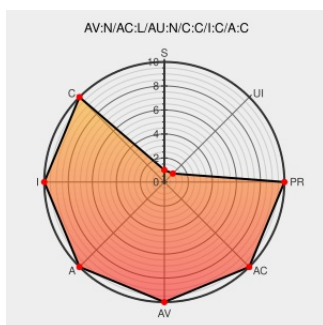


CVE-2010-1554

Published on: 05/13/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:05 PM UTC

CVE-2010-1554

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Openview Network Node Manager](#) from [Hp](#) contain the following vulnerability:

Stack-based buffer overflow in getnnmdata.exe in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allows remote attackers to execute arbitrary code via an invalid iCount parameter.

CVE-2010-1554 has been assigned by hp-security-alert@hp.com to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

SecurityFocus

www.securityfocus.com
[text/html](#)

[BUGTRAQ 20100511 ZDI-10-085: HP OpenView NNM getnnmdata.exe CGI Invalid ICount Remote Code Execution Vulnerability](#)

HP OpenView NNM getnnmdata.exe CGI Invalid ICount Remote Code Execution

www.exploit-db.com
[Proof of Concept](#)
[text/html](#)

[EXPLOIT-DB 14181](#)

CXSecurity - IDS

securityreason.com
[text/html](#)

[SREASON 8154](#)

'[security bulletin] HPSBMA02527 SSRT010098 rev.1 - HP OpenView Network Node Manager (OV NNM), Remote' - MARC

marc.info
[text/html](#)

[HP SSRT090229](#)

Zero Day Initiative

zerodayinitiative.com
[text/html](#)

[MISC zerodayinitiative.com/advisories/ZDI-10-085/](http://MISC.zerodayinitiative.com/advisories/ZDI-10-085/)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hp	Openview Network Node Manager	7.0.1	All	All	All
Application	Hp	Openview Network Node Manager	7.51	All	All	All
Application	Hp	Openview Network Node Manager	7.51	-	hp-ux	All
Application	Hp	Openview Network Node Manager	7.51	-	linux	All
Application	Hp	Openview Network Node Manager	7.51	-	solaris	All
Application	Hp	Openview Network Node Manager	7.51	-	windows	All
Application	Hp	Openview Network Node Manager	7.53	All	All	All
Application	Hp	Openview Network Node Manager	7.53	-	hp-ux	All
Application	Hp	Openview Network Node Manager	7.53	-	linux	All
Application	Hp	Openview Network Node Manager	7.53	-	solaris	All
Application	Hp	Openview Network Node Manager	7.53	-	windows	All
Application	Hp	Openview Network Node Manager	7.0.1	All	All	All
Application	Hp	Openview Network Node Manager	7.51	All	All	All
Application	Hp	Openview Network Node Manager	7.51	-	hp-ux	All
Application	Hp	Openview Network Node Manager	7.51	-	linux	All
Application	Hp	Openview Network Node Manager	7.51	-	solaris	All
Application	Hp	Openview Network Node Manager	7.51	-	windows	All
Application	Hp	Openview Network Node Manager	7.53	All	All	All
Application	Hp	Openview Network Node Manager	7.53	-	hp-ux	All
Application	Hp	Openview Network Node Manager	7.53	-	linux	All
Application	Hp	Openview Network Node Manager	7.53	-	solaris	All
Application	Hp	Openview Network Node Manager	7.53	-	windows	All
cpe:2.3:a:hp:openview_network_node_manager:7.0.1:*:*:*:*:*:						
cpe:2.3:a:hp:openview_network_node_manager:7.51:*:*:*:*:*:						
cpe:2.3:a:hp:openview_network_node_manager:7.51::-hp-ux:*:*:*:*:						
cpe:2.3:a:hp:openview_network_node_manager:7.51::-linux:*:*:*:*:						

cpe:2.3:a:hp:openview_network_node_manager:7.51:-:solaris:*:*:*:*:
cpe:2.3:a:hp:openview_network_node_manager:7.51:-:windows:*:*:*:*:
cpe:2.3:a:hp:openview_network_node_manager:7.53:*:*:*:*:*:
cpe:2.3:a:hp:openview_network_node_manager:7.53:-:hp-ux:*:*:*:*:
cpe:2.3:a:hp:openview_network_node_manager:7.53:-:linux:*:*:*:*:
cpe:2.3:a:hp:openview_network_node_manager:7.53:-:solaris:*:*:*:*:
cpe:2.3:a:hp:openview_network_node_manager:7.53:-:windows:*:*:*:*:
cpe:2.3:a:hp:openview_network_node_manager:7.0.1:*:*:*:*:*:
cpe:2.3:a:hp:openview_network_node_manager:7.51:*:*:*:*:*:
cpe:2.3:a:hp:openview_network_node_manager:7.51:-:hp-ux:*:*:*:*:
cpe:2.3:a:hp:openview_network_node_manager:7.51:-:linux:*:*:*:*:
cpe:2.3:a:hp:openview_network_node_manager:7.51:-:solaris:*:*:*:*:
cpe:2.3:a:hp:openview_network_node_manager:7.51:-:windows:*:*:*:*:
cpe:2.3:a:hp:openview_network_node_manager:7.53:*:*:*:*:*:
cpe:2.3:a:hp:openview_network_node_manager:7.53:-:hp-ux:*:*:*:*:
cpe:2.3:a:hp:openview_network_node_manager:7.53:-:linux:*:*:*:*:
cpe:2.3:a:hp:openview_network_node_manager:7.53:-:solaris:*:*:*:*:
cpe:2.3:a:hp:openview_network_node_manager:7.53:-:windows:*:*:*:*:

No vendor comments have been submitted for this CVE