



CVE-2013-6765

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

Summary

CVE	CVE-2013-6765
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-19 14:55:00 UTC
Updated	2014-05-19 19:03:00 UTC
Description	OpenVAS Manager 3.0 before 3.0.7 and 4.0 before 4.0.4 allows remote attackers to bypass the OMP authentication restric

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openvas	Openvas Manager	3.0	beta1	All	All
Application	Openvas	Openvas Manager	3.0	beta2	All	All
Application	Openvas	Openvas Manager	3.0	beta3	All	All
Application	Openvas	Openvas Manager	3.0	beta4	All	All
Application	Openvas	Openvas Manager	3.0	beta5	All	All
Application	Openvas	Openvas Manager	3.0	beta6	All	All
Application	Openvas	Openvas Manager	3.0	beta7	All	All
Application	Openvas	Openvas Manager	3.0	beta8	All	All
Application	Openvas	Openvas Manager	3.0	rc1	All	All
Application	Openvas	Openvas Manager	3.0.0	All	All	All
Application	Openvas	Openvas Manager	3.0.1	All	All	All
Application	Openvas	Openvas Manager	3.0.2	All	All	All
Application	Openvas	Openvas Manager	3.0.3	All	All	All
Application	Openvas	Openvas Manager	3.0.4	All	All	All
Application	Openvas	Openvas Manager	3.0.5	All	All	All
Application	Openvas	Openvas Manager	3.0.6	All	All	All
Application	Openvas	Openvas Manager	4.0	beta1	All	All

Application	Openvas	Openvas Manager	4.0	beta2	All	All
Application	Openvas	Openvas Manager	4.0	beta3	All	All
Application	Openvas	Openvas Manager	4.0	beta4	All	All
Application	Openvas	Openvas Manager	4.0	beta5	All	All
Application	Openvas	Openvas Manager	4.0	rc1	All	All
Application	Openvas	Openvas Manager	4.0.0	All	All	All
Application	Openvas	Openvas Manager	4.0.1	All	All	All
Application	Openvas	Openvas Manager	4.0.2	All	All	All
Application	Openvas	Openvas Manager	4.0.3	All	All	All
Application	Openvas	Openvas Manager	3.0	beta1	All	All
Application	Openvas	Openvas Manager	3.0	beta2	All	All
Application	Openvas	Openvas Manager	3.0	beta3	All	All
Application	Openvas	Openvas Manager	3.0	beta4	All	All
Application	Openvas	Openvas Manager	3.0	beta5	All	All
Application	Openvas	Openvas Manager	3.0	beta6	All	All
Application	Openvas	Openvas Manager	3.0	beta7	All	All
Application	Openvas	Openvas Manager	3.0	beta8	All	All
Application	Openvas	Openvas Manager	3.0	rc1	All	All
Application	Openvas	Openvas Manager	3.0.0	All	All	All
Application	Openvas	Openvas Manager	3.0.1	All	All	All
Application	Openvas	Openvas Manager	3.0.2	All	All	All
Application	Openvas	Openvas Manager	3.0.3	All	All	All
Application	Openvas	Openvas Manager	3.0.4	All	All	All
Application	Openvas	Openvas Manager	3.0.5	All	All	All
Application	Openvas	Openvas Manager	3.0.6	All	All	All
Application	Openvas	Openvas Manager	4.0	beta1	All	All
Application	Openvas	Openvas Manager	4.0	beta2	All	All
Application	Openvas	Openvas Manager	4.0	beta3	All	All
Application	Openvas	Openvas Manager	4.0	beta4	All	All
Application	Openvas	Openvas Manager	4.0	beta5	All	All
Application	Openvas	Openvas Manager	4.0	rc1	All	All
Application	Openvas	Openvas Manager	4.0.0	All	All	All
Application	Openvas	Openvas Manager	4.0.1	All	All	All
Application	Openvas	Openvas Manager	4.0.2	All	All	All
Application	Openvas	Openvas Manager	4.0.3	All	All	All

References			
Reference	Source	Link	Tags
[Openvas-announce] Security Releases for OpenVAS-5 and OpenVAS-6	MLIST	lists.wald.intevation.org	Vendor Advisory
OpenVAS - OpenVAS	CONFIRM	www.openvas.org	
oss-security - CVE-2013-6765 CVE-2013-6766 for OpenVAS 4.0.4/1.3.2/etc.	MLIST	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis
No vendor comments have been submitted for this CVE.			
There are currently no legacy QID mappings associated with this CVE.			

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report