



CVE-2015-0012

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

Summary

CVE	CVE-2015-0012
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-02-11 03:00:00 UTC
Updated	2018-11-20 20:29:00 UTC
Description	Microsoft System Center Virtual Machine Manager (VMM) 2012 R2 Update Rollup 4 does not properly validate the roles of

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Virtual Machine Manager	2012	r2_rollup4	All	All
Application	Microsoft	Virtual Machine Manager	2012	r2_rollup4	All	All

References

Reference	Source
Microsoft Virtual Machine Manager CVE-2015-0012 Local Privilege Escalation Vulnerability	BID
Microsoft System Center Virtual Machine Manager Lets Remote Authenticated Users Gain Elevated Privileges - SecurityTracker	SECTRA
IBM X-Force Exchange	XF
Microsoft Security Bulletin MS15-017 - Important Microsoft Docs	MS
Microsoft Visual Basic Lets Remote Users Bypass ASLR on the Target System - SecurityTracker	SECTRA
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)