



CVE-2014-3573

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2014-3573
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-18 00:55:00 UTC
Updated	2023-02-13 00:40:00 UTC
Description	The oVirt Engine backend module, as used in Red Hat Enterprise Virtualization Manager before 3.4.2, uses an "insecure D

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Enterprise Virtualization Manager	All	All	All	All

References

Reference

- Red Hat Customer Portal
- 1125795 – (CVE-2014-3573) CVE-2014-3573 oVirt Engine: XML eXternal Entity (XXE) flaw in backend module
- Red Hat Enterprise Virtualization Manager XXE Bug Lets Remote Authenticated Users Obtain Files on the Target System - SecurityTracker
- CVE-2014-3573 - Red Hat Customer Portal
- Red Hat Customer Portal
- 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)