CVE-2014-3485

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2014-3485
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-07-11 14:55:03 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The REST API in the ovirt-engine in oVirt, as used in Red Hat Enterprise Virtualization (rhevm) 3.4, allows remote authentic

Risk And Classification

Primary CVSS: v2.0 4 from nvd@nist.gov

AV:N/AC:L/Au:S/C:P/I:N/A:N

Problem Types: CWE-200 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:L/Au:S/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Enterprise Virtualization	3.4	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
Red Hat Enterprise Virtualization Manager XXE Bug Lets Remote Authenticated Users Obtain Files on the Target System - SecurityTracker
Red Hat Customer Portal
Red Hat Customer Portal
access.redhat.com | CVE-2014-3485
1107472 – (CVE-2014-3485) CVE-2014-3485 ovirt-engine-api: XML eXternal Entity (XXE) flaw
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.