



CVE-2017-7510

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

Summary

CVE	CVE-2017-7510
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-25 18:29:00 UTC
Updated	2023-02-12 23:30:00 UTC
Description	In ovirt-engine 4.1, if a host was provisioned with cloud-init, the root password could be revealed through the REST interface

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Ovirt-engine	4.1.0	-	All	All
Application	Redhat	Ovirt-engine	4.1.0	-	All	All

References

Reference	Source	Link
CVE-2017-7510 - Red Hat Customer Portal	MISC	access.redh
Red Hat Customer Portal	MISC	access.redh
1456590 – (CVE-2017-7510) CVE-2017-7510 RHV 4: ovirt-engine exposes cloud-init root password via REST API	CONFIRM	bugzilla.red
1456590 – (CVE-2017-7510) CVE-2017-7510 RHV 4: ovirt-engine exposes cloud-init root password via REST API	MISC	bugzilla.red
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)