



Rhn-proxy: rhn-satellite: rhn-proxy: information disclosure via clear-text credential transmission when accessing rhn satellite

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

Summary

CVE	CVE-2012-5562
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-12-02 19:15:11 UTC
Updated	2026-04-09 18:16:40 UTC
Description	A flaw was found in rhn-proxy. This vulnerability may allow the rhn-proxy to transmit user credentials in clear-text when it ac

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Problem Types: CWE-319 | CWE-319 Cleartext Transmission of Sensitive Information

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Secondary	6.5	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	secalert@redhat.com	Primary	8.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
3.1	CNA	CVSS	8.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
2.0	nvd@nist.gov	Primary	3.3		AV:A/AC:L/Au:N/C:P/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v2.0 Breakdown

Access Vector

Adjacent

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Satellite	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Satellite 6	Not specified	Not specified

References

Reference	Source
Bug 850953 – VUL-1: CVE-2012-5562: spacewalk: rhn-proxy: may transmit credentials over clear-text	af854a3a-2127-422b-91ae-364da260
access.redhat.com/security/cve/CVE-2012-5562	secalert@redhat.com
CVE-2012-5562 - Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da260
879369 – (CVE-2012-5562) CVE-2012-5562 rhn-proxy: may transmit credentials over clear-text	af854a3a-2127-422b-91ae-364da260
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2026-04-02T15:02:44.461Z	Reported to Red Hat.
CNA	2019-12-02T18:12:41.000Z	Made public.

Workarounds

CNA: Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

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](#)