



CVE-2008-3270

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

Summary

CVE	CVE-2008-3270
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-08-18 17:41:00 UTC
Updated	2017-09-29 01:31:00 UTC
Description	yum-rhn-plugin in Red Hat Enterprise Linux (RHEL) 5 does not verify the SSL certificate for a file download from a Red Hat

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All

References

Reference	Source
457113 – (CVE-2008-3270) CVE-2008-3270 yum-rhn-plugin: does not verify SSL certificate for all communication with RHN server	CC
Repository / Oval Repository	OV
Support	RE
Red Hat update for yum-rhn-plugin - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SE
Red Hat yum-rhn-plugin RHN Updates Denial of Service Vulnerability	BID
yum-rhn-plugin Certificate Validation Flaw Lets Remote Users Conduct Man-in-the-Middle Attacks to Prevent Updates - SecurityTracker	SE
CVE Program record	CV
NVD vulnerability detail	NV

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](#)