



CVE-2012-4556

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

Summary

CVE	CVE-2012-4556
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-01-04 22:55:00 UTC
Updated	2013-01-15 05:00:00 UTC
Description	The token processing system (pki-tps) in Red Hat Certificate System (RHCS) before 8.1.3 allows remote attackers to cause

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Certificate System	7.1	All	All	All
Application	Redhat	Certificate System	7.2	All	All	All
Application	Redhat	Certificate System	7.3	All	All	All
Application	Redhat	Certificate System	8.0	All	All	All
Application	Redhat	Certificate System	8.1	All	All	All
Application	Redhat	Certificate System	7.1	All	All	All
Application	Redhat	Certificate System	7.2	All	All	All
Application	Redhat	Certificate System	7.3	All	All	All
Application	Redhat	Certificate System	8.0	All	All	All
Application	Redhat	Certificate System	8.1	All	All	All
Application	Redhat	Certificate System	All	All	All	All

References

Reference	Source	Link
Red Hat Certificate System Multiple Cross-Site Scripting and Denial of Service Vulnerabilities	BID	www
Security Advisory SA51482 - Red Hat update for pki - Secunia	SECUNIA	secu
Red Hat Certificate System Flaws Permit Cross-Site Scripting and Denial of Service Attacks - SecurityTracker	SECTrack	www

869579 – (CVE-2012-4556) CVE-2012-4556 pki-tps: Connection reset when performing empty certificate search in TPS	MISC	bug:
Red Hat Customer Portal	REDHAT	rhn.
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.
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](#)