



CVE-2008-5082

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

Summary

CVE	CVE-2008-5082
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-01-30 19:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The verifyProof function in the Token Processing System (TPS) component in Red Hat Certificate System (RHCS) 7.1 thro

Risk And Classification

Primary CVSS: v2.0 6 from nvd@nist.gov

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

Problem Types: CWE-287 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

Single

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

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	Dogtag Certificate System	1.0	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Red Hat Certificate Server Information Disclosure and Security Bypass - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854
IBM X-Force Exchange	af854
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854
rhn.redhat.com Red Hat Support	af854
475998 – (CVE-2008-5082) CVE-2008-5082 Certificate System: missing public key challenge proof verification in the TPS component	af854
Red Hat Certificate System Security Bypass Vulnerability	af854
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.