CVE-2010-1439

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

Summary

CVE	CVE-2010-1439
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-06-07 17:12:48 UTC
Updated	2026-04-29 01:13:23 UTC
Description	yum-rhn-plugin in Red Hat Network Client Tools (aka rhn-client-tools) on Red Hat Enterprise Linux (RHEL) 5 and Fedora us

Risk And Classification

Primary CVSS: v2.0 3.6 from nvd@nist.gov

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

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	All	All	All	All

Operating System	Redhat	Enterprise Linux	5	All	All	All
Operating System	Redhat	Enterprise Linux	5	ga	server	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Application	Redhat	Rhn-client-tools	All	All	All	All
Application	Redhat	Yum-rhn-plugin	All	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
www.osvdb.org/65063	af854a3a-2127-422b-91ae-3
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-3
Red Hat Client Tools 'loginAuth.pkl' Local Security Bypass Vulnerability	af854a3a-2127-422b-91ae-3
rhn.redhat.com | Red Hat Support	af854a3a-2127-422b-91ae-3
Red Hat update for rhn-client-tools - Advisories - Community	af854a3a-2127-422b-91ae-3
IBM X-Force Exchange	af854a3a-2127-422b-91ae-3
Repository / Oval Repository	af854a3a-2127-422b-91ae-3
SecurityTracker.com Archives - Red Hat Network Client Tools Lets Local Users Obtain RHN Access Password	af854a3a-2127-422b-91ae-3
585386 – (CVE-2010-1439) CVE-2010-1439 rhn-client-tools: authorized information disclosure	af854a3a-2127-422b-91ae-3
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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