CVE-2014-0189

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

Summary

CVE	CVE-2014-0189
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-02 14:55:05 UTC
Updated	2026-05-06 22:30:45 UTC
Description	virt-who uses world-readable permissions for /etc/sysconfig/virt-who, which allows local users to obtain password for hyperv

Risk And Classification

Primary CVSS: v2.0 2.1 from nvd@nist.gov

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

Problem Types: CWE-310 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All

Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Virt-who Project	Virt-who	-	All	All	All

Vendor Declared Affected Products

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

References

Reference
1088732 – (CVE-2014-0189) CVE-2014-0189 virt-who: plaintext hypervisor passwords in world-readable /etc/sysconfig/virt-who configuration
oss-security - CVE-2014-0189: /etc/sysconfig/virt-who is world-readable (contains unencrypted passwords)
Red Hat Customer Portal
Bug 1081286 – [RFE] Cannot add unencrypted administrative credentials of Vcenter in "/etc/sysconfig/virt-who"
virt-who CVE-2014-0189 Local Information Disclosure Vulnerability
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
access.redhat.com | CVE-2014-0189
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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