CVE-2014-8169

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

Summary

CVE	CVE-2014-8169
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-03-18 16:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	automount 5.0.8, when a program map uses certain interpreted languages, uses the calling user's USER and HOME enviro

Risk And Classification

Primary CVSS: v2.0 4.4 from nvd@nist.gov

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

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Automount Project	Automount	5.0.8	All	All	All

Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All

Vendor Declared Affected Products

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

References

Reference	Sc
openSUSE-SU-2015:0475-1: moderate: Security update for autofs	af
Red Hat Customer Portal	af
Automount CVE-2014-8169 Local Privilege Escalation Vulnerability	af
Bug 1192565 – CVE-2014-8169 autofs: priv escalation via interpreter load path for program based automount maps	af
USN-2579-1: autofs vulnerability | Ubuntu	af
Oracle Linux Bulletin - October 2015	af
Bug 917977 – VUL-0: CVE-2014-8169: autofs: potential privilege escalation via interpreter load path for program-based automount maps	af
Red Hat Customer Portal	M
Red Hat Customer Portal	M
CVE-2014-8169 - Red Hat Customer Portal	M
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 and Source URL Uptime Status status.cve.report