



CVE-2014-4038

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

Summary

CVE	CVE-2014-4038
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-06-17 15:55:06 UTC
Updated	2026-05-06 22:30:45 UTC
Description	ppc64-diag 2.6.1 allows local users to overwrite arbitrary files via a symlink attack related to (1) rtas_errd/diag_support.c an

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-59 | 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	Ppc64-diag Project	Ppc64-diag	2.6.1	All	All	All

Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	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 Customer Portal	af854a3a-2127-4...
1109371 – (CVE-2014-4038, CVE-2014-4039) CVE-2014-4038 CVE-2014-4039 ppc64-diag: multiple temporary file races	af854a3a-2127-4...
Security Advisory SA60616 - SUSE update for ppc64-diag - Secunia	af854a3a-2127-4...
ppc64-diag CVE-2014-4038 Multiple Race Condition Vulnerabilities	af854a3a-2127-4...
Red Hat Customer Portal	af854a3a-2127-4...
oss-security - Re: CVE request: multiple /tmp races in ppc64-diag	af854a3a-2127-4...
[security-announce] SUSE-SU-2014:0928-1: important: Security update for	af854a3a-2127-4...
Access Denied	af854a3a-2127-4...
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.