Rsync: race condition in rsync handling symbolic links

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

Summary

CVE	CVE-2024-12747
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-01-14 18:15:25 UTC
Updated	2026-04-14 22:16:27 UTC
Description	A flaw was found in rsync. This vulnerability arises from a race condition during rsync's handling of symbolic links. Rsync's c

Risk And Classification

Primary CVSS: v3.1 5.6 MEDIUM from secalert@redhat.com

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N

EPSS: 0.000140000 probability, percentile 0.026330000 (date 2026-04-15)

Problem Types: CWE-362 | CWE-362 Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	5.6	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N
3.1	CNA	CVSS	5.6	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

ntegrity

None

Availability

None

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 0:3.4.1-2.el10 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:3.1.3-21.el8_10 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:3.2.5-3.el9 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:3.2.5-3.el9 * rpm
CNA	Red Hat	Red Hat Discovery 1.14	unaffected sha256:492e412759cf0eedfa5b557f7b0865f8864f84d0ed75e11dc
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified

References

Reference	Source	Link	Tags
access.redhat.com/security/cve/CVE-2024-12747	secalert@redhat.com	access.redhat.com	
security.netapp.com/advisory/ntap-20250131-0002	af854a3a-2127-422b-91ae-364da2661108	security.netapp.com	
access.redhat.com/errata/RHSA-2025:7050	secalert@redhat.com	access.redhat.com	
www.kb.cert.org/vuls/id/952657	af854a3a-2127-422b-91ae-364da2661108	www.kb.cert.org	
kb.cert.org/vuls/id/952657	secalert@redhat.com	kb.cert.org	
access.redhat.com/errata/RHSA-2025:2600	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/errata/RHBA-2025:6470	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:8385	secalert@redhat.com	access.redhat.com	
lists.debian.org/debian-lts-announce/2025/01/msg00008.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Aleksei Gorban "loqpa" for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-12-18T07:12:52.493Z	Reported to Red Hat.
CNA	2025-01-14T15:06:00.000Z	Made public.

Workarounds

CNA: Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

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