Rsync: --safe-links option bypass leads to path traversal

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

Summary

CVE	CVE-2024-12088
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. When using the `--safe-links` option, the rsync client fails to properly verify if a symbolic link dest

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from nvd@nist.gov

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

EPSS: 0.028870000 probability, percentile 0.863240000 (date 2026-04-15)

Problem Types: CWE-22 | CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
3.1	secalert@redhat.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version
Operating System	Almalinux	Almalinux	10.0
Operating System	Almalinux	Almalinux	8.0
Operating System	Almalinux	Almalinux	9.0
Operating System	Archlinux	Arch Linux	-
Operating System	Gentoo	Linux	-
Operating System	Nixos	Nixos	All
Operating System	Novell	Suse Linux	-
Application	Redhat	Discovery	1.14
Operating System	Redhat	Enterprise Linux	10.0
Operating System	Redhat	Enterprise Linux	6.0
Operating System	Redhat	Enterprise Linux	7.0
Operating System	Redhat	Enterprise Linux	8.0
Operating System	Redhat	Enterprise Linux	9.0
Operating System	Redhat	Enterprise Linux Eus	9.6
Operating System	Redhat	Enterprise Linux For Arm 64	8.0_aarch64
Operating System	Redhat	Enterprise Linux For Arm 64	9.0_aarch64
Operating System	Redhat	Enterprise Linux For Arm 64 Eus	9.6_aarch64
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	8.0_s390x
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	9.0_s390x
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	9.6_s390x
Operating System	Redhat	Enterprise Linux For Power Little Endian	8.0_ppc64le
Operating System	Redhat	Enterprise Linux For Power Little Endian	9.0_ppc64le
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	9.6_ppc64le
Operating System	Redhat	Enterprise Linux Server Aus	9.6
Operating System	Redhat	Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions	9.6_ppc64le
Operating System	Redhat	Enterprise Linux Update Services For Sap Solutions	9.6

Application	Redhat	Openshift Container Platform	4.0
Application	Samba	Rsync	All
Operating System	Tritondatacenter	Smartos	All

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
security.netapp.com/advisory/ntap-20250131-0002	af854a3a-2127-422b-91ae-364da2661108	security.netap
access.redhat.com/errata/RHSA-2025:7050	secalert@redhat.com	access.redhat
www.kb.cert.org/vuls/id/952657	af854a3a-2127-422b-91ae-364da2661108	www.kb.cert.o
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redha
kb.cert.org/vuls/id/952657	secalert@redhat.com	kb.cert.org
access.redhat.com/errata/RHSA-2025:2600	secalert@redhat.com	access.redhat
access.redhat.com/errata/RHBA-2025:6470	secalert@redhat.com	access.redhat
access.redhat.com/errata/RHSA-2025:8385	secalert@redhat.com	access.redhat
github.com/google/security-research/security/advisories/GHSA-p5pg-x43v-mvqj	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
access.redhat.com/security/cve/CVE-2024-12088	secalert@redhat.com	access.redhat
lists.debian.org/debian-lts-announce/2025/01/msg00008.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.or
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Jasiel Spelman (Google), Pedro Gallegos (Google), and Simon Scannell (Google) for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-12-05T21:55:22.700Z	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.