



Rsync: path traversal vulnerability in rsync

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

Summary

CVE	CVE-2024-12087
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 22:16:26 UTC
Description	A path traversal vulnerability exists in rsync. It stems from behavior enabled by the `--inc-recursive` option, a default-enable

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: 0.031890000 probability, percentile 0.869920000 (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	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	Samba	Rsync	All
Operating System	Suse	Suse Linux	-
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 6 Extended Lifecycle Support - EXTENSION	unaffected 0:3.0.6-12.el6_10.2 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 7 Extended Lifecycle Support	unaffected 0:3.1.2-12.el7_9.2 * 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 8.2 Advanced Update Support	unaffected 0:3.1.3-7.el8_2.6 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support	unaffected 0:3.1.3-12.el8_4.6 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Extended Update Support Long-Life Add-On	unaffected 0:3.1.3-12.el8_4.6 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support	unaffected 0:3.1.3-14.el8_6.9 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Telecommunications Update Service	unaffected 0:3.1.3-14.el8_6.9 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Update Services For SAP Solutions	unaffected 0:3.1.3-14.el8_6.9 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Telecommunications Update Service	unaffected 0:3.1.3-20.el8_8.4 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Update Services For SAP Solutions	unaffected 0:3.1.3-20.el8_8.4 * 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 Enterprise Linux 9.0 Update Services For SAP Solutions	unaffected 0:3.2.3-9.el9_0.4 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.2 Update Services For SAP Solutions	unaffected 0:3.2.3-19.el9_2.2 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 0:3.2.3-19.el9_4.2 * rpm
CNA	Red Hat	Red Hat Discovery 1.14	unaffected sha256:492e412759cf0eedfa5b!
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified

References

Reference	Source	Link
access.redhat.com/errata/RHSA-2025:23416	secalert@redhat.com	access.redhat.com/errata/RHSA-2025:23416
security.netapp.com/advisory/ntap-20250131-0002	af854a3a-2127-422b-91ae-364da2661108	security.netapp.com/advisory/ntap-20250131-0002
access.redhat.com/errata/RHSA-2025:7050	secalert@redhat.com	access.redhat.com/errata/RHSA-2025:7050
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com/show_bug.cgi
access.redhat.com/errata/RHSA-2025:23854	secalert@redhat.com	access.redhat.com/errata/RHSA-2025:23854
access.redhat.com/errata/RHSA-2025:23858	secalert@redhat.com	access.redhat.com/errata/RHSA-2025:23858
www.kb.cert.org/vuls/id/952657	af854a3a-2127-422b-91ae-364da2661108	www.kb.cert.org/vuls/id/952657
access.redhat.com/errata/RHSA-2025:23842	secalert@redhat.com	access.redhat.com/errata/RHSA-2025:23842
access.redhat.com/security/cve/CVE-2024-12087	secalert@redhat.com	access.redhat.com/security/cve/CVE-2024-12087
access.redhat.com/errata/RHSA-2025:23235	secalert@redhat.com	access.redhat.com/errata/RHSA-2025:23235
access.redhat.com/errata/RHSA-2025:23415	secalert@redhat.com	access.redhat.com/errata/RHSA-2025:23415
kb.cert.org/vuls/id/952657	secalert@redhat.com	kb.cert.org/vuls/id/952657
access.redhat.com/errata/RHSA-2025:2600	secalert@redhat.com	access.redhat.com/errata/RHSA-2025:2600

access.redhat.com/errata/RHSA-2025:23853	secalert@redhat.com	access.redhat
access.redhat.com/errata/RHSA-2025:23154	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/errata/RHSA-2025:23407	secalert@redhat.com	access.redhat
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
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	2024-12-05T21:23:24.139Z	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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)