Rsync: info leak via uninitialized stack contents

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

Summary

CVE	CVE-2024-12085
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 22:16:24 UTC
Description	A flaw was found in rsync which could be triggered when rsync compares file checksums. This flaw allows an attacker to ma

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from secalert@redhat.com

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

EPSS: 0.191430000 probability, percentile 0.953580000 (date 2026-04-15)

Problem Types: CWE-908 | CWE-908 Use of Uninitialized Resource

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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/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	8.8
Operating System	Redhat	Enterprise Linux Eus	9.2
Operating System	Redhat	Enterprise Linux Eus	9.4
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	9.2_aarch64
Operating System	Redhat	Enterprise Linux For Arm 64 Eus	8.8_aarch64
Operating System	Redhat	Enterprise Linux For Arm 64 Eus	9.4_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	9.2_s390x
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	8.8_s390x
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	9.4_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	8.8_ppc64le
Operating System	Redhat	Enterprise Linux For Power Little Endian	9.0_ppc64le
Operating System	Redhat	Enterprise Linux For Power Little Endian	9.2_ppc64le
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	9.4_ppc64le

Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	9.6_ppc64le
Operating System	Redhat	Enterprise Linux Server	6.0
Operating System	Redhat	Enterprise Linux Server	7.0
Operating System	Redhat	Enterprise Linux Server Aus	8.2
Operating System	Redhat	Enterprise Linux Server Aus	8.4
Operating System	Redhat	Enterprise Linux Server Aus	8.6
Operating System	Redhat	Enterprise Linux Server Aus	9.2
Operating System	Redhat	Enterprise Linux Server Aus	9.4
Operating System	Redhat	Enterprise Linux Server Aus	9.6
Operating System	Redhat	Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions	8.4_ppc64le
Operating System	Redhat	Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions	8.6_ppc64le
Operating System	Redhat	Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions	8.8_ppc64le
Operating System	Redhat	Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions	9.0_ppc64le
Operating System	Redhat	Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions	9.2_ppc64le
Operating System	Redhat	Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions	9.4_ppc64le
Operating System	Redhat	Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions	9.6_ppc64le
Operating System	Redhat	Enterprise Linux Server Tus	8.4
Operating System	Redhat	Enterprise Linux Server Tus	8.6
Operating System	Redhat	Enterprise Linux Server Tus	8.8
Operating System	Redhat	Enterprise Linux Update Services For Sap Solutions	8.4
Operating System	Redhat	Enterprise Linux Update Services For Sap Solutions	8.6
Operating System	Redhat	Enterprise Linux Update Services For Sap Solutions	9.0
Operating System	Redhat	Enterprise Linux Update Services For Sap Solutions	9.2
Operating System	Redhat	Enterprise Linux Update Services For Sap Solutions	9.6
Application	Redhat	Openshift	5.0
Application	Redhat	Openshift Container Platform	4.12
Application	Redhat	Openshift Container Platform	4.13
Application	Redhat	Openshift Container Platform	4.14
Application	Redhat	Openshift Container Platform	4.15
Application	Redhat	Openshift Container Platform	4.16
Application	Redhat	Openshift Container Platform	4.17
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_10.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 7 Extended Lifecycle Support	unaffected 0:3.1.2-12.el7_9.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:3.1.3-20.el8_10 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.2 Advanced Update Support	unaffected 0:3.1.3-7.el8_2.3 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support	unaffected 0:3.1.3-12.el8_4.3 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Telecommunications Update Service	unaffected 0:3.1.3-12.el8_4.3 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Update Services For SAP Solutions	unaffected 0:3.1.3-12.el8_4.3 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support	unaffected 0:3.1.3-14.el8_6.6 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Telecommunications Update Service	unaffected 0:3.1.3-14.el8_6.6 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Update Services For SAP Solutions	unaffected 0:3.1.3-14.el8_6.6 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Extended Update Support	unaffected 0:3.1.3-20.el8_8.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:3.2.3-20.el9_5.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:3.2.3-20.el9_5.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.0 Update Services For SAP Solutions	unaffected 0:3.2.3-9.el9_0.3 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.2 Extended Update Support	unaffected 0:3.2.3-19.el9_2.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 0:3.2.3-19.el9_4.1 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.12	unaffected 412.86.202502100314-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.13	unaffected 413.92.202503112237-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.14	unaffected 414.92.202502111902-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.15	unaffected 415.92.202501281917-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.16	unaffected v4.16.0-202501311735.p0.g2cb00
CNA	Red Hat	Red Hat OpenShift Container Platform 4.16	unaffected v4.16.0-202501311933.p0.g4246d
CNA	Red Hat	Red Hat OpenShift Container Platform 4.16	unaffected v4.16.0-202501311605.p0.g4246d
CNA	Red Hat	Red Hat OpenShift Container Platform 4.17	unaffected 417.94.202502051822-0 * rpm
CNA	Red Hat	RHOL-5.8-RHEL-9	unaffected v5.8.17-22 * rpm
CNA	Red Hat	RHOL-5.8-RHEL-9	unaffected v5.8.17-10 * rpm
CNA	Red Hat	RHOL-5.8-RHEL-9	unaffected v6.8.1-454 * rpm
CNA	Red Hat	RHOL-5.8-RHEL-9	unaffected v5.8.17-17 * rpm
CNA	Red Hat	RHOL-5.8-RHEL-9	unaffected v1.0.0-537 * rpm
CNA	Red Hat	RHOL-5.8-RHEL-9	unaffected v5.8.17-4 * rpm
CNA	Red Hat	RHOL-5.8-RHEL-9	unaffected v0.4.0-339 * rpm
CNA	Red Hat	RHOL-5.8-RHEL-9	unaffected v5.8.17-4 * rpm

CNA	Red Hat	RHOL-5.8-RHEL-9	unaffected v1.1.0-320 * rpm
CNA	Red Hat	RHOL-5.8-RHEL-9	unaffected v5.8.1-552 * rpm
CNA	Red Hat	RHOL-5.8-RHEL-9	unaffected v3.3.2-9 * rpm
CNA	Red Hat	RHOL-5.8-RHEL-9	unaffected v5.8.17-5 * rpm
CNA	Red Hat	RHOL-5.8-RHEL-9	unaffected v5.8.17-12 * rpm
CNA	Red Hat	RHOL-5.8-RHEL-9	unaffected v5.8.17-5 * rpm
CNA	Red Hat	RHOL-5.8-RHEL-9	unaffected v0.1.0-725 * rpm
CNA	Red Hat	RHOL-5.8-RHEL-9	unaffected v0.1.0-342 * rpm
CNA	Red Hat	RHOL-5.8-RHEL-9	unaffected v0.28.1-88 * rpm
CNA	Red Hat	RHOL-5.9-RHEL-9	unaffected v5.9.11-25 * rpm
CNA	Red Hat	RHOL-5.9-RHEL-9	unaffected v5.9.11-11 * rpm
CNA	Red Hat	RHOL-5.9-RHEL-9	unaffected v0.4.0-340 * rpm
CNA	Red Hat	RHOL-5.9-RHEL-9	unaffected v5.9.11-5 * rpm
CNA	Red Hat	RHOL-5.9-RHEL-9	unaffected v1.1.0-321 * rpm
CNA	Red Hat	RHOL-5.9-RHEL-9	unaffected v3.3.2-8 * rpm
CNA	Red Hat	RHOL-5.9-RHEL-9	unaffected v5.9.11-6 * rpm
CNA	Red Hat	RHOL-5.9-RHEL-9	unaffected v5.9.11-9 * rpm
CNA	Red Hat	RHOL-5.9-RHEL-9	unaffected v5.9.11-4 * rpm
CNA	Red Hat	RHOL-5.9-RHEL-9	unaffected v0.1.0-724 * rpm
CNA	Red Hat	RHOL-5.9-RHEL-9	unaffected v0.1.0-341 * rpm
CNA	Red Hat	RHOL-5.9-RHEL-9	unaffected v0.34.1-30 * rpm
CNA	Red Hat	Compliance Operator 1	unaffected sha256:4953a7ea865ff38a4fe19d5

References

Reference	Source	Link
access.redhat.com/errata/RHSA-2025:0884	secalert@redhat.com	access.redhat
access.redhat.com/errata/RHSA-2025:2701	secalert@redhat.com	access.redhat
access.redhat.com/errata/RHSA-2025:1451	secalert@redhat.com	access.redhat
security.netapp.com/advisory/ntap-20250131-0002	af854a3a-2127-422b-91ae-364da2661108	security.netap
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redha
access.redhat.com/errata/RHSA-2025:21885	secalert@redhat.com	access.redhat
access.redhat.com/errata/RHSA-2025:0688	secalert@redhat.com	access.redhat
access.redhat.com/errata/RHSA-2025:0714	secalert@redhat.com	access.redhat
access.redhat.com/errata/RHSA-2025:0324	secalert@redhat.com	access.redhat
access.redhat.com/errata/RHSA-2025:0787	secalert@redhat.com	access.redhat
access.redhat.com/errata/RHSA-2025:0637	secalert@redhat.com	access.redhat

www.kb.cert.org/vuls/id/952657	af854a3a-2127-422b-91ae-364da2661108	www.kb.cert.o
access.redhat.com/errata/RHSA-2025:1225	secalert@redhat.com	access.redhat
access.redhat.com/errata/RHSA-2025:0774	secalert@redhat.com	access.redhat
kb.cert.org/vuls/id/952657	secalert@redhat.com	kb.cert.org
access.redhat.com/errata/RHSA-2025:0325	secalert@redhat.com	access.redhat
access.redhat.com/errata/RHSA-2025:1123	secalert@redhat.com	access.redhat
access.redhat.com/security/cve/CVE-2024-12085	secalert@redhat.com	access.redhat
access.redhat.com/errata/RHSA-2025:0790	secalert@redhat.com	access.redhat
access.redhat.com/errata/RHSA-2025:0885	secalert@redhat.com	access.redhat
access.redhat.com/errata/RHSA-2025:1120	secalert@redhat.com	access.redhat
access.redhat.com/errata/RHSA-2025:1128	secalert@redhat.com	access.redhat
access.redhat.com/errata/RHBA-2025:6470	secalert@redhat.com	access.redhat
access.redhat.com/errata/RHSA-2025:1227	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-2025:1242	secalert@redhat.com	access.redhat
access.redhat.com/errata/RHSA-2025:0849	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	2024-12-05T12:06:36.594Z	Reported to Red Hat.
CNA	2025-01-14T15:06:00.000Z	Made public.

Workarounds

CNA: Seeing as this vulnerability relies on information leakage coming from the presence of data in the uninitialized memory of the `sum2` buffer, a potential mitigation involves compiling rsync with the `-ftrivial-auto-var-init=zero` option set. This mitigates the issue because it initializes the `sum2` variable's memory with zeroes to prevent uninitialized memory disclosure.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report