Rsync: rsync server leaks arbitrary client files

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

Summary

CVE	CVE-2024-12086
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 flaw was found in rsync. It could allow a server to enumerate the contents of an arbitrary file from the client's machine. Th

Risk And Classification

Primary CVSS: v3.1 6.8 MEDIUM from nvd@nist.gov

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

EPSS: 0.009140000 probability, percentile 0.759120000 (date 2026-04-15)

Problem Types: CWE-390 | CWE-390 Detection of Error Condition Without Action

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N
3.1	secalert@redhat.com	Secondary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:N/A:N
3.1	CNA	CVSS	6.1	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

ntegrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Almalinux	Almalinux	10.0	-	All	All
Operating System	Almalinux	Almalinux	8.0	-	All	All
Operating System	Almalinux	Almalinux	9.0	-	All	All
Operating System	Archlinux	Arch Linux	-	All	All	All
Operating System	Gentoo	Linux	-	All	All	All
Operating System	Nixos	Nixos	All	All	All	All
Operating System	Redhat	Enterprise Linux	10.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	Redhat	Openshift Container Platform	4.0	All	All	All
Application	Samba	Rsync	All	All	All	All
Operating System	Suse	Suse Linux	-	All	All	All
Operating System	Tritondatacenter	Smartos	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 0:3.4.1-2.el10 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified	Not specified

References

Reference	Source	Link
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redha
security.netapp.com/advisory/ntap-20250131-0002	af854a3a-2127-422b-91ae-364da2661108	security.netap

security.netapp.com/advisory/ntap-20250131-0002	af854a3a-2127-422b-91ae-364da2661108	security.netap
www.kb.cert.org/vuls/id/952657	af854a3a-2127-422b-91ae-364da2661108	www.kb.cert.o
kb.cert.org/vuls/id/952657	secalert@redhat.com	kb.cert.org
access.redhat.com/errata/RHBA-2025:6470	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-2024-12086	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	2024-12-05T00:00:00.000Z	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.