EVIDEN
an atos business

Security Bulletin

Vulnerabilities in rsync

Author(s)	:	**Eviden PSIRT**
Reference	:	**PSIRT-1854**
Created	:	**03 January 2025**
Version	:	**0.4**
Status	:	**Neutralization**
TLP Classification	:	**CLEAR**
Document date	:	**17 February 2025**
Keywords	:	**CVE-2024-12084 CVE-2024-12085 CVE-2024-12086 CVE-2024-12087 CVE-2024-12088 CVE-2024-12747**

TLP:CLEAR

Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

FOR PUBLIC USE

List of changes

Version	Date	Description
0.1	2024/12/24	Initial Eviden version
0.2	2025/01/06	CVE description updated
0.3	2025/01/27	TLP changed fr, added information about errata. Changed information that Slurm will be unpatched
0.4	2025/02/17	TLP changed for CLEAR

Executive summary

Security researchers from Google's Cloud Vulnerability found 5 vulnerabilities in rsync. Vulnerabilities affecting all Linux distros, many other unix-like distros. SSH probably is also affected. Vulnerabilities affecting Rsync lower than 3.3.0 Users are strongly urged to update their Rsync installations immediately to the latest patched version. Patches are available at the official Rsync website and the Samba project website. It's also crucial to ensure that any software using Rsync as a backend is updated to address these vulnerabilities.

Vulnerability Info

CVE No.	CVSS Score	Type of Vulnerability
CVE-2024-12084	9.8	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2024-12085	7.5	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVE-2024-12086	6.1	AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:N/A:N
CVE-2024-12087	6.5	AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N
CVE-2024-12088	6.5	AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N
CVE-2024-12747	6.3	AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N

CVE-2024-12084

A heap-based buffer overflow flaw was found in the rsync utility. This issue is due to improper handling of attacker-controlled checksum lengths (s2length) in the code. When MAX_DIGEST_LEN exceeds the fixed SUM_LENGTH (16 bytes), an attacker can write out of bounds in the sum2 buffer.

CVE-2024-12085

A vulnerability was found in rsync when the daemon compares file checksums. This flaw allows an attacker to manipulate the checksum length (s2length) to cause a comparison between a checksum and uninitialized memory and leak one byte of uninitialized stack data at a time.

CVE-2024-12086

A flaw was found in the rsync package, where a server can leak the contents of an arbitrary file from the client's machine. This issue occurs while starting the copy process from files from the client. During this process, a maliciously crafted rsync server can generate invalid communication token and a checksum from the data the attacker wants to compare. This will trigger the client to ask the server to resend the data, then the malicious server can use this as a signal if the checksum sent was correctly. A malicious server is then able to determine the contents of the target file byte by byte.

CVE-2024-12087

A path traversal vulnerability exists in rsync which affects the - option, a default-enabled option for many flaws that can be enabled by the server even if not explicitly enabled by the client. When using the -inc-recursive option, a lack of proper symlink verification coupled with deduplication checks occurring on a per-file-list basis could allow a server to write files outside of the client's intended destination directory. A malicious server could remotely trigger this by exploiting symbolic links named after valid client directories/paths, thereby reducing the integrity of the client.

CVE-2024-12088

When using the --safe-links option, rsync fails to properly verify if a symbolic link destination contains another symbolic link with it. This results in a path traversal vulnerability, which may lead to arbitrary file write outside the desired directory.

CVE-2024-12747

This vulnerability arises from a race condition during rsync's handling of symbolic links in specific scenarios. This flaw allows attackers to manipulate symbolic links while rsync runs, leading to unintended data access.

Affected products

Products	Fixed version	Status	Comments
Rsync	3.3.0	Affected	affects versions lower than 3.3.0

Although Eviden tries to provide accurate and complete information, Eviden shall not be liable if the above table is incomplete or erroneous. During its vulnerability analysis process, the information in this document is subject to change without notice to reflect new results of this analysis.

TBD (to be defined) indicates that a new technical state fixing the vulnerabilities is under study.

Unpatched means that the vulnerability is presumably present, but there is no plan to provide a fix. This can be investigated on demand.

List of HPC Management products

Products	Fixed version	Status	Remaining vulnerabilities
Slurm	Unpatched	Affected	fix is depending on rsync update

Recommendations
Eviden recommends applying rsync updates as soon as they are made available.

Available Vendor Patches
Redhat has published validated rsync patches (see References section).

Available Workarounds
Slurm is depending on rsync for some operations and could therefore be indirectly affected by the vulnerability.

Available Mitigations
No mitigation identified.

Available Exploits/PoC
Eviden is not aware of any exploitation of the reported vulnerabilities.

References
1. https://kb.cert.org/vince/comm/case/vuln/4510/
2. https://access.redhat.com/security/cve/cve-2024-12084
3. https://access.redhat.com/security/cve/cve-2024-12085
4. https://access.redhat.com/security/cve/cve-2024-12086
5. https://access.redhat.com/security/cve/cve-2024-12087
6. https://access.redhat.com/security/cve/cve-2024-12088
7. https://access.redhat.com/security/cve/cve-2024-12747

8. https://access.redhat.com/errata/RHSA-2025:0325
9. https://access.redhat.com/errata/RHSA-2025:0324

Glossary of terms

Term	Description
Mitigation	Refers to a setting, common configuration, or general best-practice, existing in a default state that could reduce the severity of exploitation of a vulnerability
Neutralization	The neutralization phase is the decision-making process during which the risk posed by an incident is evaluated.
PoC	Proof of Concept
Remediation	The remediation phase ends with the delivering of a qualified solution/update fixing the vulnerability without regression.
TI	Threat Intelligence
TLP	Traffic Light Protocol (TLP) FIRST Standards Definitions and Usage Guidance — Version 2.0. https://www.first.org/tlp/
Workaround	Refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update

About this document

Eviden continuously monitors the security of its products. This Security Bulletin is shared under the constraints of the FIRST Traffic Light Protocol version 2.0 (TLP) to bring the attention of owners of the potentially affected Eviden products. Eviden recommends that all product owners determine whether the described situation is applicable to their individual case and take appropriate action.

Although Eviden tries to provide accurate and complete information, Eviden shall not be liable for technical or editorial errors contained in this Bulletin. The information is provided “as is” without warranty of any kind. To the extent permitted by the Law, neither Eviden nor its affiliates, subcontractors or suppliers will be liable for incidental damages, downtime cost, lost profits, damages relating to the procurement of substitute products or services, or damages for loss of data, or software restoration. Product and company names mentioned herein may be trademarks of their respective owners.

The information in this document is subject to change without notice. The version of this document will be incremented according to the changes:

- Neutralization security bulletins are numbered 0.x
- Privately disclosed Remediation security bulletins are numbered 1.x
- Publicly disclosed Remediation security bulletins are numbered 2.x

Updated versions of this document can be found on:

- https://support.bull.com/ols/product/security/psirt

About Atos

Atos is a global leader in digital transformation with 105,000 employees and annual revenue of c. € 11 billion. European number one in cybersecurity, cloud and high-performance computing, the Group provides tailored end-to-end solutions for all industries in 69 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

About Eviden[1]

Eviden is a next-gen technology leader in data-driven, trusted and sustainable digital transformation with a strong portfolio of patented technologies. With worldwide leading positions in advanced computing, security, AI, cloud and digital platforms, it provides deep expertise for all industries in more than 47 countries. Bringing together 53,000 world-class talents, Eviden expands the possibilities of data and technology across the digital continuum, now and for generations to come. Eviden is an Atos Group company with an annual revenue of c. € 5 billion.

[1] Eviden business is operated through the following brands: AppCentrica, ATHEA, BullSequana, Cloudamize, Cloudreach, Cryptovision, DataSentics, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, IDnomic, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Trustway, Visual BI, Worldgrid, X-Perion.