Customers rate Sysdig top CNAPP in Customers' Choice category within Gartner® VOC report LEARN MORE

BACK TO BLOG

Detecting and mitigating CVE-2024-12084: rsync remote code execution

BY SYSDIG THREAT RESEARCH TEAM - JANUARY 17, 2025

TOPICS: THREAT RESEARCH

SHARE:

On Tuesday, January 14, 2025, a set of vulnerabilities were announced that affect the “**rsync**” utility. rsync allows files and directories to be flexibly transferred locally and remotely. It is often used for deployments and backup purposes. In total, 6 vulnerabilities were announced to the OSS Security mailing list. The most severe vulnerability, CVE-2024-12084, may result in remote code execution. This post will cover how to detect and mitigate CVE-2024-12084.

At the time of this writing, no proof of concept has been released, nor has there been any indication of active exploitation.

(UPDATE) On February 19, 2025 additional information was published about how to trigger the vulnerabilities. No exploit code was included, but this information will assist in development.

Vulnerabilities

CVE-2024-12084 **(CVSS 9.8) – Heap overflow that could lead to remote code execution**

CVE-2024-12085 (CVSS 7.5) – Information leak

CVE-2024-12086 (CVSS 6.1) – Information leak

CVE-2024-12087 (CVSS 6.5) – Path traversal

CVE-2024-12088 (CVSS 6.5) – Path traversal

CVE-2024-12747 (CVSS 5.6) – Symbolic link race condition

Customers rate Sysdig top CNAPP in Customers' Choice category within Gartner® VOC report LEARN MORE

features of rsync is that it will only transfer files that have changed or are missing. This allows users to keep files in sync across different directories, both locally and remotely. Since it can be used remotely, it can be listening on port 873 (TCP) as a daemon process. When running as a daemon, it is called “**rsyncd**.”

rsync can also be run remotely on demand. In this scenario, a user would set up “**rsync**” to listen on the remote server, and then use rsync locally to start the transfer. To learn more about “**rsync**” and what it can do, here is a useful guide.

Detecting CVE-2024-12084

A heap overflow vulnerability was reported on January 14, 2025, which can lead to remote code execution in the targeted process. This class of vulnerability allows an attacker to redirect the execution of a process to an area of memory they control, where they have placed malicious code. One strategy for detecting this is to monitor the process for unusual behavior, such as command executions.

Falco is well suited to this task as it has full visibility into the system calls made by “**rsync**.” In our detection, we will monitor the process for suspicious command executions. For example, rsync shouldn’t execute many commands (**iptables, mongodump, curl**, …) or other system commands. There is a use case where rsync can execute a shell using the “**-e**” option, which can allow for a privilege escalation if the binary is SETUID.

# This macro can be modified for other, non-shell, commands.

```
- macro: shell_binaries_arg_filename

  condition: (  evt.arg.filename endswith "/ash" or evt.arg.filename endswith "/bash"
or evt.arg.filename endswith "/csh" or evt.arg.filename endswith "/ksh" or
evt.arg.filename endswith "/sh" or evt.arg.filename endswith "/tcsh" or
evt.arg.filename endswith "/zsh" or evt.arg.filename endswith "/dash" )

- rule: Possible Remote Code Execution using rsync

  desc: This rule detects rsync and rsyncd processes executing unexpected binaries,
which may indicate arbitrary command execution through CVE-2024-12084.

  condition: evt.type in ( execve, execveat ) and evt.dir=> and proc.name in ( rsync,
rsyncd ) and shell_binaries_arg_filename

  output: The %proc.name process was seen executing unexpected binary
%evt.arg.filename which may indicate arbitrary command execution through the rsync or
potential vulnerability exploitation (proc.exepath=%proc.exepath
evt.arg.filename=%evt.arg.filename fd.name=%fd.name user.name=%user.name
proc.name=%proc.name proc.pname=%proc.pname
image=%container.image.repository:%container.image.tag proc.cmdline=%proc.cmdline
evt.res=%evt.res proc.pcmdline=%proc.pcmdline user.uid=%user.uid
user.loginuid=%user.loginuid user.loginname=%user.loginname
container.name=%container.name)
```

Customers rate Sysdig top CNAPP in Customers' Choice category within Gartner® VOC report LEARN MORE

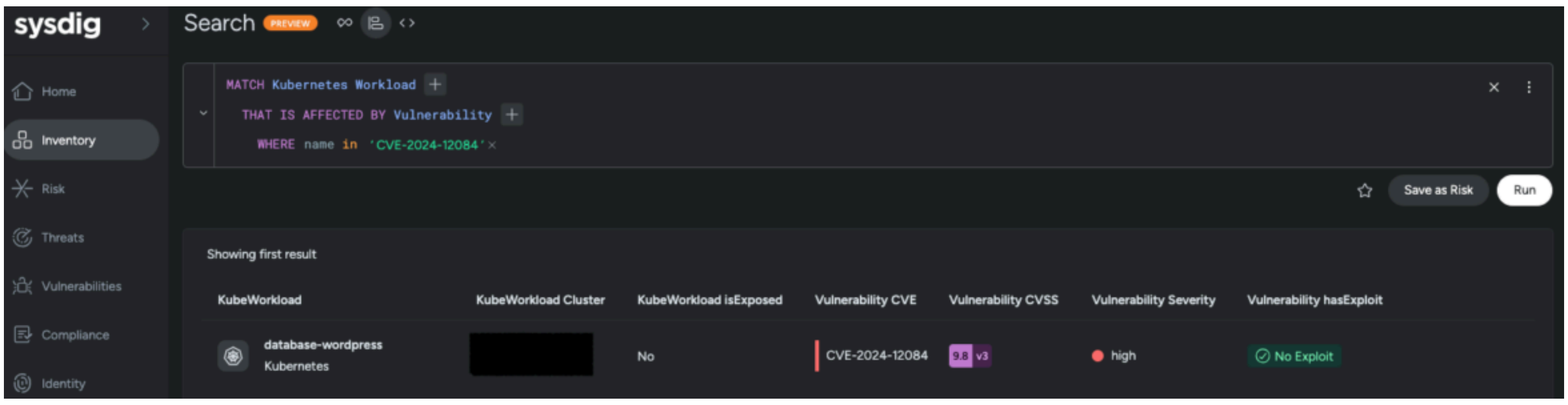
Sysdig Secure customers automatically have this rule in the **Sysdig Runtime Notable Events** policy.

Mitigating CVE-2024-12084

The versions affected by the heap overflow are: ***rsync >= 3.2.7 and < 3.4.0***

Organizations should prioritize remediating this vulnerability and patch all affected systems immediately. Remediation entails upgrading all instances of rsync in an environment to version 3.4.0, as that version will address all of the announced CVEs.

Using Sysdig Secure's Inventory, users can query all workloads affected by CVE-2024-12084. This is enabled by a flexible query language, which is one of multiple ways users can search through their inventory.



```
MATCH Kubernetes Workload
  THAT IS AFFECTED BY Vulnerability
    WHERE name in 'CVE-2024-12084'
```

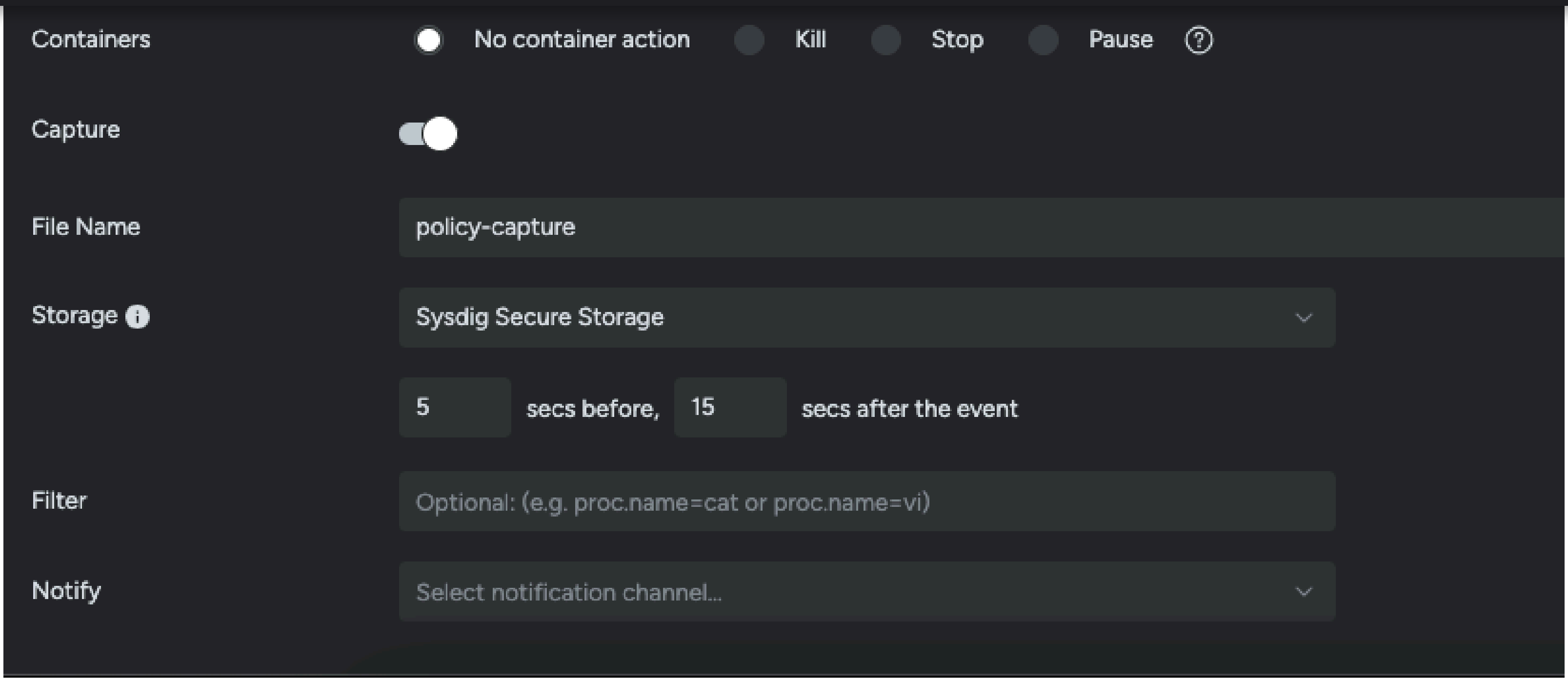
Showing first result

KubeWorkload	KubeWorkload Cluster	KubeWorkload isExposed	Vulnerability CVE	Vulnerability CVSS	Vulnerability Severity	Vulnerability hasExploit
database-wordpress Kubernetes	[redacted]	No	CVE-2024-12084	9.8 v3	● high	No Exploit

If patching isn't immediately possible, ensuring none of the instances of rsync are exposed to the Internet is another step that can reduce the risk. By default, rsync listens on TCP port 873. The port should be blocked or restricted at the firewall or security group. This course of action may still leave exposure to internal attacks though.

For Sysdig Secure customers, the platform offers several options for response if the above rule is triggered. "**Kill Process**" can be used to terminate the shell that the attacker launches. Or for a more complete response in a containerized environment, "**Kill Container**" can be used to eliminate the entire workload. For deep forensic review, a syscall capture can be taken automatically.

Customers rate Sysdig top CNAPP in Customers' Choice category within Gartner® VOC report LEARN MORE



Containers ● No container action ○ Kill ○ Stop ○ Pause

Capture: on

File Name: policy-capture

Storage: Sysdig Secure Storage

5 secs before, 15 secs after the event

Filter: Optional: (e.g. proc.name=cat or proc.name=vi)

Notify: Select notification channel...

Conclusion

rsync is a common file synchronization utility that, according to Bleeping Computer, is present on over 600k systems exposed to the Internet. Of the six new vulnerabilities, CVE-2024-12084 may allow for remote code execution. Using Sysdig Secure, which is powered by open source Falco, this type of attack can be instantly detected and a response can be quickly initiated.

Subscribe and get the latest updates

SUBMIT →

□ Also keep me informed of Sysdig news + updates

Customers rate Sysdig top CNAPP in Customers' Choice category within Gartner® VOC report LEARN MORE

sysdig

Sitemap

sysdig

® Copyright 2025 Sysdig, Inc.

Privacy Policy

Privacy Choices

Subprocessors

Trust Center

Change Consent