



TRY FOR FREE



TuxCare PR Team

CATEGORIES

[TuxCare News](#)

[KernelCare Enterprise](#)

[Extended Lifecycle Support](#)

[Linux Tips & Patch Management](#)

[Malware & Exploits](#)

[Live Patching Education](#)

[Cybersecurity News](#)

Follow Us On Social

[TuxCare Blog News](#)

TuxCare Team identifies CVE-2021-38604, a new vulnerability in glibc

August 13, 2021



The TuxCare Team is responsible for performing in-depth analyses of new CVEs. This is done for every new CVE that pops up, which affects, directly or indirectly, the Linux ecosystem. We check to see if the distributions we provide services for are affected. When one such CVE does affect the supported distributions, the Team members roll up their sleeves and start digging into the code.

While performing this work on CVE-2021-33574, Nikita Popov, one of our Team members, identified a problem with the upstream glibc. It turns out that it is possible to cause a situation where a segmentation fault could be triggered in a specific code path within the library. This can, in turn, lead to the application using the library to crash, resulting in a Denial-of-Service issue.

Bear in mind that glibc provides the main system primitives and is linked with most, if not all, other Linux applications, including other language compilers and interpreters. It is the second most important component of a system after the Kernel itself.

This problem was introduced with the original upstream fix for [CVE-2021-33574](#), specifically in the file mq_notify.c:

```
@@ -133,8 +133,11 @@ helper_thread (void *arg)
    (void) __pthread_barrier_wait (&notify_barrier);
    }
    else if (data.raw[NOTIFY_COOKIE_LEN - 1] == NOTIFY_REMOVED)
-   /* The only state we keep is the copy of the thread attributes. */
-   free (data.attr);
+   {
+   /* The only state we keep is the copy of the thread attributes. */
+   pthread_attr_destroy (data.attr);
+   free (data.attr);
+   }
```

While the free() call is immune to NULL pointers being passed to it, pthread_attr_destroy() is not. It was possible to identify two situations where the Linux Kernel would use the message NOTIFY_REMOVED while passing copied thread attributes along the way in the data.attr field. Unfortunately, a host application is able to pass a NULL value there if it wants glibc to spawn a thread with default attributes. In this case, glibc would dereference a NULL pointer in pthread_attr_destroy, leading to a crash of the entire process.

Following responsible disclosure guidelines, both the vulnerability and code fix were submitted to the team responsible for glibc, and a CVE was requested at Mitre (CVE-2021-38604). In glibc, it was assigned as bug 28213. This has already been incorporated into upstream glibc.

A new test was also submitted to glibc's automated test suite to pick up this situation and prevent it from happening in the future. Sometimes, changes in unrelated code paths can lead to behaviours changing elsewhere in the code and the programmer not being aware of it. This test will catch this situation.

For context, the family of "mq_" functions provide POSIX compliant message queue API functionality and asynchronous notifications of incoming messages and are typically used for inter-process communications.

Relevant links:

<https://sourceware.org/git/?p=glibc.git;a=commit;h=42d359350510506b87101cf77202f6c9b790cb>

https://sourceware.org/bugzilla/show_bug.cgi?id=28213




Expert knowledge of Linux security tips, live patching education, and Cybersecurity news.

Stay updated with the latest news and announcements from TuxCare.com


Work Email*

Related Articles




The Bugs Behind the Vulnerabilities...

November 14, 2022




Cybersecurity insurance and fine print...

June 29, 2022



IT Automation With Live Patching


June 20, 2022



UPDATE

KernelCare ePortal updated - version...


June 16, 2022



UPDATE

KernelCare agent update - version...


June 2, 2022



UPDATE


KernelCare ePortal updated - version...

May 26, 2022




The Bugs Behind the Vulnerabilities...

November 14, 2022




Cybersecurity insurance and fine print...

June 29, 2022



IT Automation With Live Patching


June 20, 2022



UPDATE

KernelCare ePortal updated - version...


June 16, 2022



UPDATE

KernelCare agent update - version...

June 2, 2022



UPDATE

KernelCare ePortal updated - version...

May 26, 2022

Resources



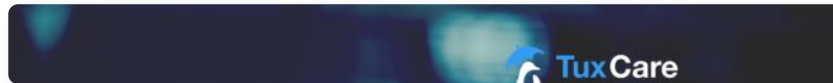
[State of Enterprise Linux Cybersecurity ...](#)

[Read More](#) →



[Dangerous remotely exploitable vulnerability ...](#)

[Read More](#) →



[Securing confidential research data ...](#)

[Read More](#) →



[State of Enterprise Vulnerability Detection ...](#)

[Read More](#) →



[Demand for Rapid Risk Elimination for ...](#)

[Read More](#) →



[TuxCare Free Raspberry Pi Patching](#)



TRY FOR FREE



[KernelCare IoT](#)
[QEMU/Care](#)
[DBCare](#)
[Extended Lifecycle Support](#)
[Linux Support Services](#)

Resources

[Blog](#)
[Changelog](#)
[CVE Dashboard](#)

About

[About Us](#)
[News & Press](#)
[Resources](#)
[Contact Us](#)
[Careers](#)
[Legal](#)
[Vulnerability Reporting](#)

Contact Us

1-800-220-3540
sales@tuxcare.com

