CVE Status | Contact Us | English

TuxCare

php2shell patches (CVE-2026-109618 and CVE-2026-109619) for EOL PHP are out now. With sales replies slower than usual due to high demand, the fastest route to patched packages is to **buy ELS for Runtimes online**. | **Read the patch FAQ**

Blog > Category > Live Patching Education

Guarding Against a glibc Vulnerability: A Security Guide

October 2, 2023 - 📖 5 min



Author:
Chris DeMars
Senior Developer Advocate

Go straight to an AI summary of this blog post instead ⟶

The GNU C Library, also called glibc, is a fundamental component of the Linux-based operating systems. It offers essential functions that programs need to work properly on your system. The glibc library has been around since 1992, and it's maintained by the GNU project. A glibc

vulnerability is a flaw or weakness in this library that can be exploited by malicious actors to compromise your system's security. These flaws can appear as buffer overflows, memory corruption, use-after-free, and other software issues.

Attackers might quickly exploit these weaknesses, so it's essential to comprehend and safeguard your systems. Attackers gain the ability to run malicious programs, steal sensitive data, and obtain unauthorized access to your system when a vulnerability is successfully exploited.

In this blog post, we will look at the critical security vulnerabilities discovered in glibc and provide best practices and tools for mitigating the potential risks.

Critical glibc Vulnerability Examples

CVE-2022-23218

In glibc up to version 2.34, the deprecated compatibility function svcunix_create in the sunrpc module copied its path argument on the stack without validating its length. This resulted in a buffer overflow vulnerability, potentially leading to a denial of service or arbitrary code execution (if stack protector is not enabled).

CVE-2022-23219

In glibc up to version 2.34, the deprecated compatibility function clnt_create in the sunrpc module copied its hostname argument onto the stack without performing sufficient length validation. This resulted in a buffer overflow vulnerability, potentially leading to a denial of service or arbitrary code execution (if stack protector is not enabled).

CVE-2023-25139

The sprintf function in glibc 2.37 has a buffer overflow vulnerability in some situations with the correct buffer size. This problem is unrelated to CWE-676. The issue arises when attempting to write a padded, thousands-separated string representation of a number into a buffer allocated precisely to accommodate that number's string representation. For instance, in cases like padding "1,234,567" to a length of 13 characters, the overflow occurs, exceeding the buffer boundaries by two bytes.

CVE-2021-35942

Within the GNU C Library (glibc) up to version 2.33, a vulnerability exists in the wordexp function. When invoked with a maliciously crafted pattern from an untrusted source, this function may lead to a system crash or unauthorized memory access within the parse_param function located in posix/wordexp.c. Consequently, this flaw could result in a denial of service or unauthorized disclosure of sensitive information.

CVE-2021-33574

The mq_notify function in glibc versions 2.32 and 2.33 was identified with a use-after-free vulnerability. This vulnerability occurs when the function continues to utilize the notification thread attributes object, which is provided through its struct sigevent parameter, even after the caller has freed it. It can potentially result in a denial of service, causing the application to crash, or potentially lead to other unspecified adverse impacts.

If you're wondering how these risks might differ for other libraries, our musl vs glibc article covers that in detail.

Zenbleed Vulnerability: A New Emerging Concern

As we assess vulnerabilities like glibc, it's also important to consider the zenbleed vulnerability that has been recently identified. While this vulnerability isn't directly tied to glibc, its ability to affect system integrity through similar buffer overflows and improper handling of memory operations has raised significant concern among Linux administrators and security professionals. The zenbleed vulnerability serves as a reminder that even subtle flaws in system libraries can lead to serious exploits if not properly addressed.

Best Practices for Linux Admins Against a glibc Vulnerability

Regular Updates

The best defense against glibc vulnerabilities is to keep your system updated. Linux distributions frequently release security updates and patches to fix known vulnerabilities, so install these updates as soon as possible.

Continuous Monitoring

Monitor your systems for suspicious activities and audit user activity for logs and records of actions taken on your computer systems and networks. This includes activities like logins, file accesses, system configuration changes, network connections, and more. Staying alert to both system-level exploits and authentication vulnerabilities is essential for maintaining a secure environment, especially in multi-user or enterprise setups.

Use Security Tools

Perform regular scanning for out-of-date shared libraries and vulnerabilities to identify and address potential weaknesses. TuxCare provides a free tool called uChecker to detect vulnerable libraries utilized by various applications.

Visit the uChecker GitHub page to learn how to scan for outdated libraries using uChecker.

Patch Management

An effective patch management strategy is crucial for ensuring robust security with timely patching. Delaying critical patches can adversely put your system at high risk, potentially leading to vulnerability exploitation.

Therefore, utilize automated patching tools like LibCare that automate vulnerability patching so you always receive patches on schedule. Additionally, LibCare offers live patching, allowing you to deploy security patches without server reboots or downtime.

TuxCare for Enterprise Live Patching Services

LibCare is an add-on tool for KernelCare Enterprise, which provides enterprise live patching services for most major Linux distributions, including Ubuntu, Debian, RHEL, CentOS, AlmaLinux, Oracle Linux, Cloud Linux, and more.

With KernelCare and LibCare working together, you can ensure the maximum protection of your Linux systems, including the shared libraries, like glibc and OpenSSL, which are prone to attacks.

It's easy to get started with LibCare. Simply add LibCare to your current KernelCare Enterprise subscription to start patching your shared libraries.

The large number of servers that rely on Linux-based operating systems makes a glibc vulnerability a serious concern. Don't compromise on glibc security or disrupt your operations any longer. With LibCare from TuxCare, improve the security posture of your company and enjoy the peace of mind that comes with automated, non-disruptive library patching.

To find out more about how LibCare can revolutionize your company's security strategy, get in touch with our experts right away.

Table of Contents

Get the open-source security answers you need

Ask Us a Question

Join Our Popular Newsletter

Join 4,500+ Linux & Open Source Professionals!

2X A MONTH. NO SPAM.

TuxCare

Your open-source stack, secure and enterprise-ready from first install through post-end of life with long-term patching, compliance, automation, and expert support.

Spring® is a trademark of Broadcom Inc. and/or its subsidiaries.

OpenSSF and the OpenSSF logo design are trademarks of The Linux Foundation. See openssf.org for more information.

© 2026 All rights reserved. TuxCare Inc.

Services

- SecureChain
- Endless Lifecycle Support
- KernelCare
- TuxCare Enterprise Support

Resources

- Changelog
- CVE Dashboard

About Us

- About TuxCare
- Careers
- Legal
- Cybersecurity Certifications
- Vulnerability Reporting

Contact Us

- Contact us
- 1-800-220-3540
-

Member of OpenSSF | Member of OpenJS Foundation | Member of OASIS OPEN | Member of CoSAI | Authorized CVE Numbering Authority (CNA)


CYBER SECURITY EXCELLENCE AWARDS
WINNER
2023
GOLD
MERIT AWARDS
Information Security
TuxCare
GOLD
GLOBAL INFOSEC AWARDS
WINNER
CYBER DEFENSE MAGAZINE
2024
SILVER
2026
WINNER
CYBER SECURITY
EXCELLENCE AWARDS
SUMMIT INTERNATIONAL AWARDS
DMA
2025 Winner
SILVER
2025 STEVIE WINNER
AMERICAN BUSINESS AWARDS
GLOBAL INFOSEC AWARDS
WINNER
CYBER DEFENSE MAGAZINE
2025
2026
AVA DIGITAL AWARDS
PLATINUM WINNER
TuxCare
The International Business Awards 2026 Winner