CVE Status | Contact Us |

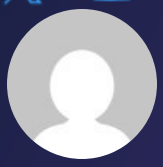
TuxCare

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 > Uncategorized

Vulnerability in iconv identified by TuxCare Team (CVE-2021-43396)

November 9, 2021 - 📖 4 min



Author:

TuxCare PR Team

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

Iconv is a library used to convert between different character encodings and is part of a core group of tools and libraries used to perform basic level tasks called glibc (GNU C Library). According to the venerable glibc

documentation, it enables the conversion of characters between 150 different character sets.

During regular work on TuxCare's Extended Lifecycle Support (ELS) service, where patches are created or backported to older Linux distributions that are past their end-of-life date, the team identified a previously unknown vulnerability in a code path inside iconv. But, of course, finding the bug is just half the work, so a fix was also developed and submitted upstream.

Patches for systems covered by ELS are already available for deployment.

The actual vulnerability happens when a specific conversion is triggered; namely, a conversion from ISO-2022-JP-3 could cause a spurious NUL character to be emitted. This could be trivially triggered by passing an escape sequence that switches the active character set. Depending on the use case, an extra NUL character received by a caller application could cause data corruption or inconsistent behaviour.

This bug was introduced as part of Bugfix 27256, as this check:

```
data->__statep->__count != ASCII_set
```

that was added by that bugfix behaves as if '', the NUL character, is queued and proceeds to emit it in the output.

When asked if he thought that the bug was currently exploitable, Nikita Popov, the team member behind the discovery, commented, "This case can be caused by a special use pattern of glibc. This is somewhat similar

to our previous bug (and is native to all libraries due to their nature: a shared library is as vulnerable as a host application being unlucky enough to utilize an unfortunate set of library calls in a specific sequence)."

This is another of TuxCare's contributions to upstream projects and also another vulnerability identified by the same team member, following one identified in glibc some weeks ago.

In keeping with industry best practices on responsible disclosure of vulnerabilities, upstream developers were notified. Additionally, a patch to correct the underlying issue was also submitted to the appropriate project repository. Because of the security implications implicit in an issue that can potentially cause data integrity problems, a CVE was requested and assigned, CVE-2021-43396. The existence of a CVE entry should hasten the incorporation of the fixed version in widespread Linux distributions.

Redhat already assigned a 7.5 CVSS v3 base score while assessing its impact on RHEL 6 to 8. NIST also assigned a 7.5 score, meaning that the vulnerability has a High risk/impact. Vulnerability prioritization for patching operations should take this information into account when preparing upcoming maintenance windows.

The ever-growing number of vulnerabilities found is a visible aspect of more and more researchers and developers going over the code – open-source code. While more vulnerabilities tend to mean more work for IT teams, the upside is that finding these issues before they are actually exploited is the best possible outcome.

The TuxCare Team will continue its work ensuring Linux distributions old and new are kept secure, with a strong commitment to open source and upstream projects.

If you would like to know more about TuxCare, its Extended Lifecycle Support service or Linux Support Service, you can find details here.

[Update 11/11 – In the interest of transparency, the status of the CVE is being disputed. While the bug has been acknowledged and the fix solves the issue, the attack vector required to exploit this is mentioned as being application-specific – the application calling iconv would have to pass the values in a specific order – rather than iconv-specific. You can find more information about this in the CVE description here https://nvd.nist.gov/vuln/detail/CVE-2021-43396. This is an example of the review process around bug submission working in the open source ecosystem. This post will be updated with further developments if/when they happen.]

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.

Terms of Use | Privacy Policy Hub | DMCA Notice | Legal |

Do Not Sell or Share My Personal Information

