XENFORO / PATH TRAVERSAL · 08 SEPT 2026

CVE-2026-74239: Windows path traversal in style imports

A backslash path escaped XenForo's style extraction directory on Windows.

POST VIEW RENDERED SOURCE HEX

ADDRESS | MARKDOWN

000000000042700 0
000000000042707 E
000000000042708 F1
000000000042711 C
000000000042712 D
000000000042719 F
000000000042720 D5
000000000042721 FE
000000000042722 8
000000000042723 4
000000000042726 E
000000000042728 A5
000000000042732 2

Skip to debugger view

Xenforo 2.3.12 build 2031270 did not treat backslashes as path separators when validating filenames in imported style archives. On Windows, an ACP administrator with the delegated `style` permission could write an archive member outside the temporary extraction directory.

Technical details

The importer rejected forward-slash traversal sequences but left backslashes unchanged. Windows interpreted those backslashes as directory separators during extraction.

An archive member can use a path such as:

```
upload/..\..\..\style-archive-sentinel.php
```

Reproduction

1. Run XenForo on Windows with PHP ZIP support enabled.
2. an ACP account with the delegated `style` permission.

0000000000427358

3. Create a style archive containing the traversal member shown above.

00000000004273BB

4. Import the archive through the normal style-import action.

00000000004273C1

5. Request `/style-archive-sentinel.php` from the web server.

0000000000427434

00000000004274A7

The importer wrote the archive member into the web root, where the web server executed it as PHP.

00000000004274BE

Impact

00000000004274F2

A delegated style administrator could write files to locations writable by the web-server process. If the web root is writable, the uploaded PHP file can execute when requested; otherwise, writes remain limited to the process's filesystem permissions.

00000000004274FC

0000000000427508

Xenforo corrected archive-path validation in 2.3.13.

References

- CVE record
- PoC
- VulnCheck advisory
- Xenforo 2.3.13 release

0000000000427000 · 25 RENDERED LINES · 1702 UTF-8 BYTES IN .WEB.RCE

.WEB.RCE · ADDRESSES ARE UTF-8 BYTE OFFSETS

AU: IDLE VIEW: POST VIEW