mLniumm Update README.md

4bf7014 · 3 days ago

READM...	Update READ...	3 days ago

README

CVE-2025-28074

[Suggested description] phpList prior to 3.6.3 is vulnerable to Cross-Site Scripting (XSS) due to improper input sanitization in lt.php. The vulnerability is exploitable when the application dynamically references internal paths and processes untrusted input without escaping, allowing an attacker to inject malicious JavaScript.

[Additional Information] This vulnerability is exploitable only when the application references internal paths dynamically. If an attacker can influence the path parameter or a similar reference mechanism, they can inject malicious input, leading to reflected XSS. The issue arises from the lack of proper input sanitization in lt.php, which fails to escape user-supplied parameters before rendering them in the response. Proper input validation and output encoding are required to mitigate this issue.

[Vulnerability Type] Cross Site Scripting (XSS)

[Vendor of Product] phpList

About

No description, website, or topics provided.

Readme

Activity

0 stars

ng

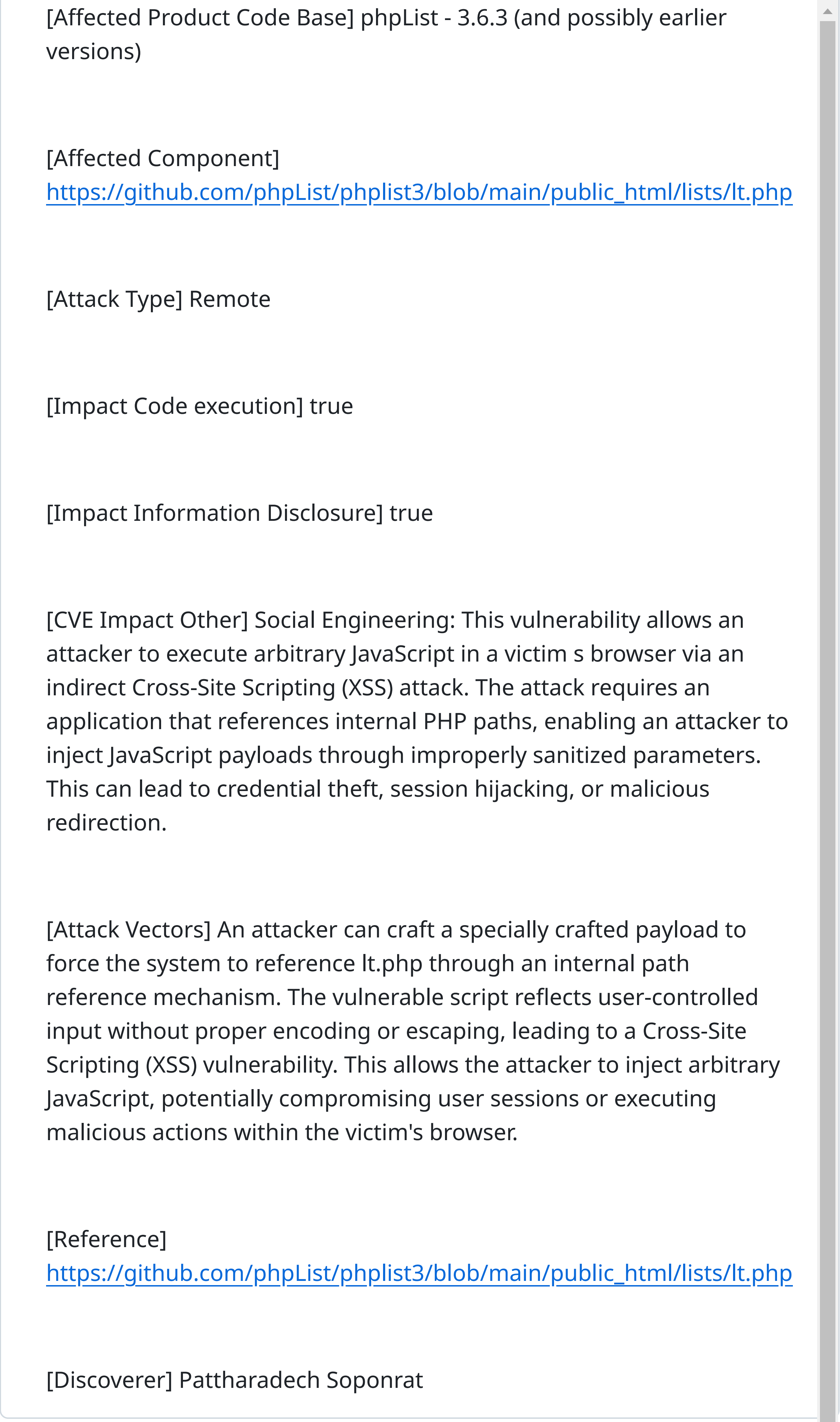
Report repository

Releases

No releases published

Packages

No packages published



[Affected Product Code Base] phpList - 3.6.3 (and possibly earlier versions)

[Affected Component] https://github.com/phpList/phplist3/blob/main/public_html/lists/lt.php

[Attack Type] Remote

[Impact Code execution] true

[Impact Information Disclosure] true

[CVE Impact Other] Social Engineering: This vulnerability allows an attacker to execute arbitrary JavaScript in a victim s browser via an indirect Cross-Site Scripting (XSS) attack. The attack requires an application that references internal PHP paths, enabling an attacker to inject JavaScript payloads through improperly sanitized parameters. This can lead to credential theft, session hijacking, or malicious redirection.

[Attack Vectors] An attacker can craft a specially crafted payload to force the system to reference lt.php through an internal path reference mechanism. The vulnerable script reflects user-controlled input without proper encoding or escaping, leading to a Cross-Site Scripting (XSS) vulnerability. This allows the attacker to inject arbitrary JavaScript, potentially compromising user sessions or executing malicious actions within the victim's browser.

[Reference] https://github.com/phpList/phplist3/blob/main/public_html/lists/lt.php

[Discoverer] Pattharadech Soponrat