mLniumm Update README.md

0c55239 · 3 days ago

README... Update READ... 3 days ago

README

CVE-2025-28073

[Suggested description] phpList 3.6.3 is vulnerable to Reflected Cross-Site Scripting (XSS) via the /lists/dl.php endpoint. An attacker can inject arbitrary JavaScript code by manipulating the id parameter, which is improperly sanitized.

[Vulnerability Type] Cross Site Scripting (XSS)

[Vendor of Product] phpList

[Affected Product Code Base] phpList - 3.6.15 (and possibly earlier versions)

[Affected Component] phpList /lists/dl.php, phpList 3.6.15 (and possibly earlier versions)

[Attack Type] Remote

[CVE Impact Other] Session Hijacking, Credential Theft, Phishing Attacks, Arbitrary JavaScript Execution

[Attack Vectors] This vulnerability is exploitable via a crafted URL containing malicious JavaScript code. A remote attacker can trick a victim into clicking a specially crafted link containing an XSS payload. When the victim accesses the vulnerable /lists/dl.php endpoint, the payload executes in their browser context. This may allow the attacker to steal session cookies, perform actions on behalf of the victim, or inject malicious content into the affected phpList instance.

[Reference]

https://github.com/phpList/phplist3

https://cve.mitre.org

https://www.exploit-db.com

[Discoverer] Pattharadech Soponrat