XSS in ShortDescription extension

Moderate **alistair3149** published **GHSA-mgcp-qw2r-6832** on Jan 24

Package

php **mediawiki/short-description** (Composer)

Affected versions	Patched versions
<2.3.3	2.3.4

Description

> On a wiki that has the ShortDescription enabled, XSS can be triggered on any page or the page with the action=info parameter, which displays the shortdesc property. This is acheived using the wikitext `{{SHORTDESC:<img src=x onerror=alert()>}}` . This is due to the function `sanitize()` in ParserHooks.php which returns `trim( html_entity_decode( strip_tags( $shortDesc ), ENT_QUOTES, 'utf-8' ) );` This strips HTML tags, of which there are none in the payload due to being encoded representations, and then the encoded entities are decoded to the actual characters. It's not clear to me why `html_entity_decode` is called or what this function is trying to achieve, I think it makes more sense to just do `trim( htmlspecialchars( $shortDesc );` .
>
> Note: this won't apply retroactively to page props that already exist in the DB, so it wouldn't fix the vulnerability in the case that someone had already exploited it.

Severity

Moderate **4.7** / 10

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	Required
Scope	Changed
Confidentiality	None

Integrity	Low
Availability	None

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N

CVE ID

CVE-2022-21710

Weaknesses

CWE-79

Credits

Dylsss