WordPress DirectoriesPro 1.3.45 Cross Site Scripting

Authored by Jack Misiura

Posted Dec 11, 2020

WordPress DirectoriesPro plugin version 1.3.45 suffers from multiple cross site scripting vulnerabilities.

tags | exploit, vulnerability, xss
advisories | CVE-2020-29303, CVE-2020-29304
SHA-256 | 6aa12eb5e2a30f4c4d114b32f8b866bc1a6a86a0191f2dd3043d5c986c598b92 **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
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=%2Fdirectories%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


-----------

Title: Self-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-2020-29304

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 column names when importing a malicious CSV file,
allowing for HTML or JavaScript injection.



2. PoC

On a WordPress installation with a vulnerable DirectoriesPro plugin import a CSV file containing the following
in the header:

'term<b>" autofocus onfocus={alert('Complex\u0020XSS');alert(document.cookie);}//'"


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
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat	150 files
Ubuntu	68 files
LiquidWorm	23 files
Debian	16 files
malvuln	11 files
nu11secur1ty	11 files
Gentoo	9 files
Google Security Research	6 files
Julien Ahrens	4 files
T. Weber	4 files

File Tags

ActiveX	(932)
Advisory	(79,754)
Arbitrary	(15,694)
BBS	(2,859)
Bypass	(1,619)
CGI	(1,018)
Code Execution	(6,926)
Conference	(673)
Cracker	(840)
CSRF	(3,290)
DoS	(22,602)
Encryption	(2,349)
Exploit	(50,359)
File Inclusion	(4,165)
File Upload	(946)
Firewall	(821)
Info Disclosure	(2,660)
Intrusion Detection	(867)
Java	(2,899)
JavaScript	(821)
Kernel	(6,291)
Local	(14,201)
Magazine	(586)
Overflow	(12,419)
Perl	(1,418)
PHP	(5,093)
Proof of Concept	(2,291)
Protocol	(3,435)
Python	(1,467)
Remote	(30,044)
Root	(3,504)
Ruby	(594)
Scanner	(1,631)
Security Tool	(7,777)
Shell	(3,103)
Shellcode	(1,204)
Sniffer	(886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX	(426)
Apple	(1,926)
BSD	(370)
CentOS	(55)
Cisco	(1,917)
Debian	(6,634)
Fedora	(1,690)
FreeBSD	(1,242)
Gentoo	(4,272)
HPUX	(878)
iOS	(330)
iPhone	(108)
IRIX	(220)
Juniper	(67)
Linux	(44,315)
Mac OS X	(684)
Mandriva	(3,105)
NetBSD	(255)
OpenBSD	(479)
RedHat	(12,469)
Slackware	(941)
Solaris	(1,607)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

Site Links
News by Month
News Tags
Files by Month
File Tags
File Directory

About Us
History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By
Rokasec

Follow us on Twitter

Subscribe to an RSS Feed