b2evolution CMS 6.11.6 Cross Site Scripting

Authored by Nakul Ratti, Soham Bakore

Posted Feb 10, 2021

b2evolution CMS version 6.11.6 suffers from multiple cross site scripting vulnerabilities.

tags | exploit, xss
advisories | CVE-2020-22839, CVE-2020-22841
SHA-256 | 9bc033021181cc828f78a45246fdbf842d7af5b01e9360d87e262f8067d9e475 Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: *Reflected XSS in b2evolution CMS 6.11.6 via tab3
parameter in evoadm.php*
# CVE : *CVE-2020-22839*
# Date: 10/02/2021
# Exploit Author: Nakul Ratti, Soham Bakore
# Vendor Homepage: https://b2evolution.net/
# Software Link:
https://b2evolution.net/downloads/6-11-6-stable?download=12405
# Version: 6.11.6
# Tested on: latest version of Chrome, Firefox on Windows and Linux


Vulnerable File:
-------------------------
http://host/evoadm.php

Vulnerable Issue:
-------------------------
Tab3 parameter has no input validation.

-------------------------Proof of Concept-----------------------
Steps to Reproduce:

1. Send the following URL *http://HOST/evoadm.php <http://host/evoadm.php>?*
*.ctrl=comments&filter=restore&tab3=123%22onmouseover=%22alert(document.domain)%22&blog=1&blog=1*
to
the logged in victim using any social engineering technique.
2. When an unsuspecting user with high privileges opens this URL, XSS will
be triggered  which will execute the malicious javascript payload in users
browser.
3. The vulnerable parameter in this case is "*tab3*".



------

# Exploit Title: b2evolution 6.11.6 - 'plugin name' Stored XSS
# Date: 09/02/2021
# Exploit Author: Soham Bakore, Nakul Ratti
# Vendor Homepage: https://b2evolution.net/
# Software Link: https://b2evolution.net/downloads/6-11-6-stable?download=12405
# Version: 6.11.6
# Tested on: latest version of Chrome, Firefox on Windows and Linux
# CVE : CVE-2020-22841


-------------------------Proof of Concept-----------------------

1. Login with an account having high privileges
2. Navigate to System -> Plugins and select any plugin
3. Change the plugin name and enter the following payload  "><svg/onload=alert(123)> in the name parameter
4. Payload gets stored in the database
5. The payload gets executed after the victim checks the plugin page.
6. This vulnerability needs high privilege and can affect other users with similar privileges
```

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

© 2022 Packet Storm. All rights reserved.

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