BigBlueButton 2.3 / 2.4.7 Cross Site Scripting

Authored by Rick Verdoes, Danny de Weille | Site pentests.nl

Posted Jul 1, 2022

BigBlueButton versions 2.3, prior to 2.4.8, and prior to 2.5.0 suffer from a persistent cross site scripting vulnerability.

tags | exploit, xss
advisories | CVE-2022-31064
SHA-256 | c68ede95337b08934eceb60e7e3ded22f6717375681d84eac96231f4c47ee8b1 Download | Favorite | View

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
CVE-2022-31064 - Stored Cross-Site Scripting in BigBlueButton.

=========================

Exploit Title: Stored Cross-Site Scripting (XSS) in BigBlueButton

Product: BigBlueButton

Vendor: BigBlueButton

Vulnerable Versions: 2.3, <2.4.8, <2.5.0

Tested Version: 2.4.7

Advisory Publication: Jun 22, 2022

Latest Update: Jun 22, 2022

Vulnerability Type: Cross-Site Scripting [CWE-79]

CVE Reference: CVE-2022-31064

CVSS Severity: High

CVSS Score: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N
Impact score: 7.2

Credit: Rick Verdoes & Danny de Weille (Hackify | pentests.nl)
=========================


I. BACKGROUND

-------------------------
BigBlueButton is an open source web conferencing system designed for online meetings and online learning.
BigBlueButton is a tool used by instructors and teachers, which helps them access to Learning Management
Systems, engagement tools and analytics.

II. VULNERABILITY
-------------------------
Users in meetings with private chat enabled are vulnerable to a cross site scripting attack in affected
versions. The attack occurs when the attacker (with a XSS payload in the name) starts a chat. in the victim's
client the JavaScript will be executed. This issue has been addressed in version 2.4.8 and 2.5.0. There are no
known workarounds for this issue.

III. Proof of Concept
-------------------------
<img x onerror=alert()>

IV. References
-------------------------
Security advisory https://pentests.nl/pentest-blog/stored-xss-in-bigbluebutton/
Patched on BigBlueButton 2.5 (https://github.com/bigbluebutton/bigbluebutton/pull/15067)
Patched on BigBlueButton 2.4 (https://github.com/bigbluebutton/bigbluebutton/pull/15090)
```


File Archive: November 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			

Top Authors In Last 30 Days

- Red Hat 186 files
- Ubuntu 52 files
- Gentoo 44 files
- Debian 27 files
- Apple 25 files
- Google Security Research 14 files
- malvuln 10 files
- nu11secur1ty 6 files
- mjurczyk 4 files
- George Tsimpidas 3 files

File Tags

- ActiveX (932)
- Advisory (79,557)
- Arbitrary (15,643)
- BBS (2,859)
- Bypass (1,615)
- CGI (1,015)
- Code Execution (6,913)
- Conference (672)
- Cracker (840)
- CSRF (3,288)
- DoS (22,541)
- Encryption (2,349)
- Exploit (50,293)
- File Inclusion (4,162)
- File Upload (946)
- Firewall (821)
- Info Disclosure (2,656)

File Archives

- November 2022
- October 2022
- September 2022
- August 2022
- July 2022
- June 2022
- May 2022
- April 2022
- March 2022
- February 2022
- January 2022
- December 2021
- Older

Systems

- AIX (426)
- Apple (1,926)

Intrusion Detection (866)
Java (2,888)
JavaScript (817)
Kernel (6,255)
Local (14,173)
Magazine (586)
Overflow (12,390)
Perl (1,417)
PHP (5,087)
Proof of Concept (2,290)
Protocol (3,426)
Python (1,449)
Remote (30,009)
Root (3,496)
Ruby (594)
Scanner (1,631)
Security Tool (7,768)
Shell (3,098)
Shellcode (1,204)
Sniffer (885)
Spoof (2,165)
SQL Injection (16,089)
TCP (2,377)
Trojan (685)
UDP (875)
Virus (661)
Vulnerability (31,104)
Web (9,329)
Whitepaper (3,728)
x86 (946)
XSS (17,478)
Other

BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,620)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,118)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,339)
Slackware (941)
Solaris (1,607)
SUSE (1,444)
Ubuntu (8,147)
UNIX (9,150)
UnixWare (185)
Windows (6,504)
Other

packet storm

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