BigBlueButton - Stored XSS in username (CVE-2022-31064)

From: Rick Verdoes via Fulldisclosure <fulldisclosure () seclists org>
Date: Tue, 28 Jun 2022 08:48:20 +0000

```
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)


_______________________________________________
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: https://seclists.org/fulldisclosure/
```


⬅ By Date ➡ ⬅ By Thread ➡

Current thread:

BigBlueButton - Stored XSS in username (CVE-2022-31064) ***Rick Verdoes via Fulldisclosure (Jun 30)***

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