BigBlueButton E-mail Validation Bypass

2020.11.25

Seccops (https://cxsecurity.com/author/Seccops/1/) (TR)

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

CVE: **CVE-2020-29043 (https://cxsecurity.com/cveshow/CVE-2020-29043/)**

CWE: **CWE-862 (https://cxsecurity.com/cwe/CWE-862)**

CVSS Base Score: **5/10**
Exploitability Subscore: **10/10**
Attack complexity: **Low**
Confidentiality impact: **None**
Availability impact: **None**

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

```
# Title: BigBlueButton E-mail Validation Bypass
# Date: 24.11.2020
# Author: Seccops (https://seccops.com)
# Vendor Homepage: bigbluebutton.org
# Version: 2.2.29 and previous versions
# CVE: CVE-2020-29043


=== Summary ===
An issue was discovered in BigBlueButton through 2.2.29. When at attacker is able to view an "account_activations/edit?token=" URI, the a
ttacker can create an approved user account associated with an email address that has an arbitrary domain name.


=== Description ===

Steps:
The verification token used in mail activation is sent with the GET method, so this token information is also seen by the attacker. Mail
verification can be performed with the token information obtained.

1) Create a new user account on the portal and enter an email address of your choice (arbitrary). https://imgur.com/a/gkHIRld

2) Login to the created account. https://imgur.com/a/ZdwZTYg

3) After logging in, you will see the screen below. Copy the token in the link "https://site.com/b/account_activations/edit?token=TOKEN_I
S_HERE" and replace it with "TOKEN_IS_HERE" and go to the link. https://imgur.com/a/Mo8Fsqc

4) Thus, you will see that your account has been approved. https://imgur.com/a/YaBrT1w

The attacker can arbitrarily register on the portal with the e-mail address of a company he wants and use the user account by unauthorize
d approval of that e-mail address.


=== Impact ===
Social engineering attacks can be made with various scenarios, crimes can be committed and these crimes remain in the approved mail accou
nt.
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2020110211)

Tı

Lul

Vote for this issue: 4 0

100%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)