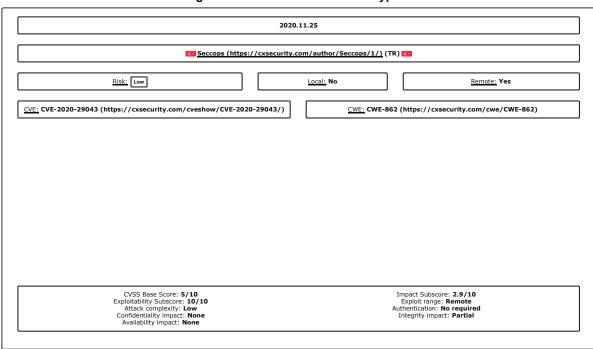
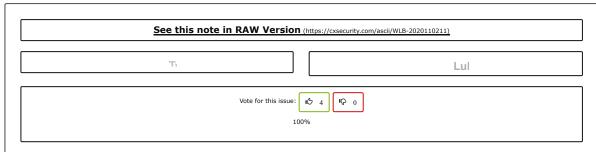
## **BigBlueButton E-mail Validation Bypass**



# 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 === 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/YaBrTlw 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.



Comment it here.		
Nick (*)		
Nick		
Email (*)		
Email		
Video		
Link to Youtube		
Text (*)		

Copyright 2022, cxsecurity.com