

Презентация по работе 3-D (НФИ-2)

Защита интеграционной платформы

Козлов В.П. Гэинэ А. Шуваев С. Джахангиров И.З Хватов М.Г.

Российский университет дружбы народов им. Патриса Лумумбы, Москва, Россия

Докладчик

- Козлов В.П., Гэинэ А., Шуваев С., Джахангиров И.З, Хватов М.Г.
- НФИбд-02-22
- Российский университет дружбы народов

Цель работы

Отработать сценарий: Защита интеграционной платформы

Задание

1. Обнаружить Bitrix vote RCE на Bitrix Server.
2. Устранить уязвимость путём отклонения всех запросов к директории vote.
3. Устранить последствие (Deface). Восстанавливаем бэкап сайта.
4. Обнаружить GitLab RCE на узле GitLab.

5. Зайти в панель администратора, ужесточить регистрацию. Удалить неизвестных пользователей.
6. Устранить последствие (Gitlab meterpreter). Убиваем сессию нарушителя.
7. Обнаружить WSO2 API-Manager RCE на узле MS API Manager.
8. Изменить параметр загрузки ресурсов в конфиг файле.
9. Устранить последствие (WSO Web User). Удалить нового привилегированного пользователя. Удалить бэкдор

На сайте ViPNet IDS NS просмотрели атакованные активы и суть атак

The screenshot displays the ViPNet IDS NS web interface. On the left is a navigation menu with sections like Monitoring, Management, and System Management. The main area is divided into two panes. The left pane shows a table of events for the last 24 hours, with columns for ID, Date and time, IP, Event code, Rule name, Class, and Priority. The right pane provides a detailed view of a selected event (ID 3121915), including its analysis rule, description, and a list of vulnerabilities.

ID	Date and time	IP	Event code	Rule name	Class	Priority
17:42:43.303 10/...	3049121	1	AM POLICY Requests Suspici...	non-standard-protocol	TC	
17:42:42.976 10/...	3001217	1	AM POLICY Requests Suspici...	non-standard-protocol	TC	
17:42:33.567 10/...	3049137	1	AM INFO Possible SSH succe...	bad-unknown	TC	
17:42:33.285 10/...	3227008	1	ET SCAN Potential SSH Scan...	attempted-recon	TC	
17:41:20.503 10/...	3121915	1	ET POLICY Executable and IL...	policy-violation	TC	
17:41:10.305 10/...	2034567	1	ET INFO curl User-Agent to D...	bad-unknown	TC	
17:41:10.305 10/...	3105345	1	AM CURRENT_EVENTS HTTP...	trojan-activity	TC	
17:41:04.028 10/...	3129327	1	ET POLICY Executable and IL...	policy-violation	TC	
17:41:04.026 10/...	2034567	1	ET INFO curl User-Agent to D...	bad-unknown	TC	
17:40:30.321 10/...	3171405	1	AM EXPLOIT Generic Comm...	web-application-attack	TC	
17:40:30.321 10/...	3203254	1	AM EXPLOIT Generic Comm...	web-application-attack	TC	
17:40:30.321 10/...	3105389	1	AM EXPLOIT Generic Comm...	web-application-attack	TC	
17:40:30.321 10/...	3171403	1	AM EXPLOIT Generic Comm...	web-application-attack	TC	
17:40:30.321 10/...	2025808	1	ET EXPLOIT php script base6...	attempted-user	TC	

Event 17:41:20.503 10/30/2025

Event Source Destination Packet

Analysis rule

Class: policy-violation
Group: policy
Name: ET POLICY Executable and linking format (ELF) file download var1

Description: This rule detects information security policy violations

Text: alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg: "ET POLICY Executable and linking format (ELF) file download var1"; flow: established; content: "0F01" /fast_pattern; content: "00 00 00 00 00 00 00 00"; distance: 6; flowbits: set; ET.ELFDownload/reference; url: web.archive.org/web/20131114024152/https://www.thea.us.edu.au/~cristina/students/david/honours/Thesis96/tf.htm; reference: url: doc.emergingthreats.net/bin/view/Main/2000418; classtype: policy-violation; sid: 3121915; rev: 6; metadata: affected_asset dst, affected_product generic_linux, affected_vendor generic_linux, attack_target Client_Endpoint, created_at 2010_07_30, tag A.M.A.R.M.A, tag T1190, tias, category Info, updated_at 2017_02_03)

Description of vulnerabilities: url: web.archive.org/web/20131114024152/https://www.thea.us.edu.au/~cristina/students/david/honours/Thesis96/tf.htm; url: doc.emergingthreats.net/bin/view/Main/2000418

Рис. 1: Атакованные ip-адреса

Добавили карточку инцидента “Bitrix vote RCE” (рис. [-@fig:100])

Добавление инцидента

Название ⓘ
Bitrix vote rce

Дата и время события ⓘ
30.10.2025 17:42

Источник ⓘ
195.239.174.11 (Kali) x

Поражённые активы ⓘ
10.10.1.33 (Bitrix CMS) x

Описание ⓘ
нарушитель может удаленно записать произвольные файлы в уязвимую систему, а также выполнить произвольную команду в записанном файле, используя небезопасную десериализацию

Рекомендации ⓘ
Закреть уязвимость можно следующими способами: добавить в исходный файл /var/www/html/bitrix/tools/vote/uf.php код, ограничивающий POST-запросы; создать по пути

Индикаторы компрометации ⓘ
еживаемые policy-violation и php-скрипт эксплойты

Прикрепить файл ⓘ
Перетяните файл в эту область или

Рис. 2: Карточка инцидента “Bitrix vote RCE”

Добавили карточку инцидента “GitLab RCE” (рис. [-@fig:200])

Добавление инцидента

Название ⓘ	Дата и время события ⓘ
GitLab RCE	30.10.2025 17:43
Источник ⓘ	Поражённые активы ⓘ
10.10.1.33 (Bitrix CMS) ×	10.10.2.18 (GitLab) ×
Описание ⓘ	Рекомендации ⓘ
Workhorse передает файлы в библиотеку <u>ExifTool</u> , которая удаляет из них метаданные. Библиотека <u>ExifTool</u> различает файлы не по расширению, а по их контенту и подбирает соответствующий фильтр.	2) активация функции подтверждения создания аккаунта администратором <u>GitLab</u> (предварительно необходимо удалить аккаунты, созданные нарушителем).
Индикаторы компрометации ⓘ	
ли в списке пользователей в админ панели гитлаба	
Прикрепить файл ⓘ	
gitlab-attempted-admin.pcap ×	
Выберите файл	

Рис. 3: Карточка инцидента “GitLab RCE”

Добавили карточку инцидента “WSO2 API-Manager RCE” (рис. [-@fig:300])

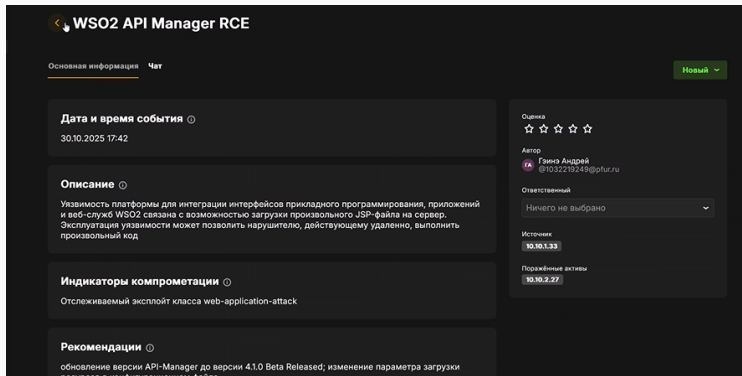
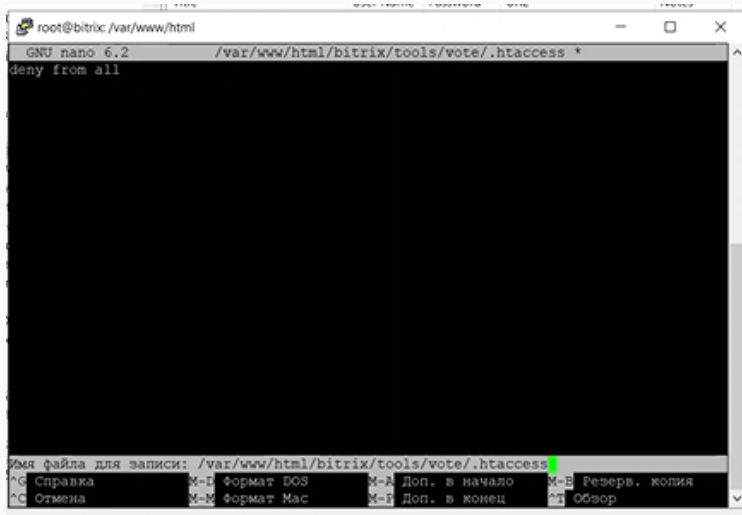


Рис. 4: Добавили карточку инцидента “WSO2 API-Manager RCE”

Bitrix vote RCE. Устранить возможность путем отклонения всех запросов к директории vote (рис. [-@fig:003])

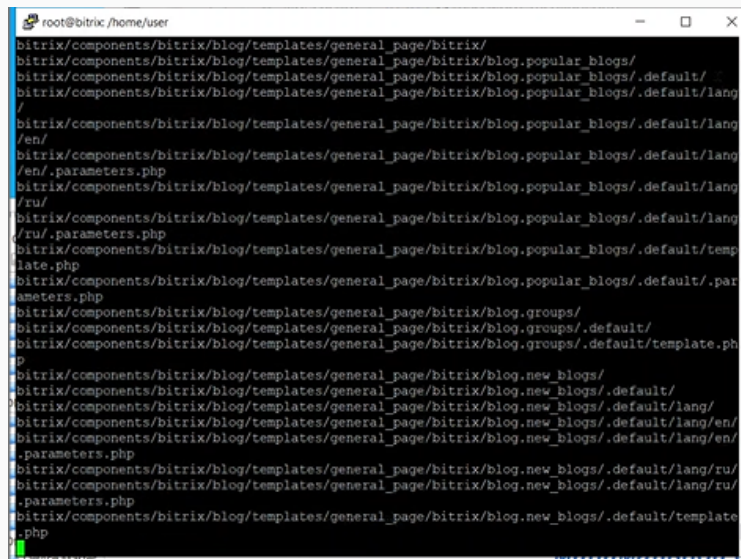


```
root@bitrix: /var/www/html
GNU nano 6.2 /var/www/html/bitrix/tools/vote/.htaccess *
deny from all

Имя файла для записи: /var/www/html/bitrix/tools/vote/.htaccess
^G Справка      М-В формат DOS  М-А Доп. в начало М-В Резерв. копия
^C Отмена       М-М формат Mac  М-Е Доп. в конец  ^П Обзор
```

Рис. 5: .htaccess

Bitrix vote RCE. Восстанавливаем бэкап сайта (рис. [-@fig:004])



```
root@bitrix:/home/user
bitrix/components/bitrix/blog/templates/general_page/bitrix/
bitrix/components/bitrix/blog/templates/general_page/bitrix/blog.popular_blogs/
bitrix/components/bitrix/blog/templates/general_page/bitrix/blog.popular_blogs/.default/
bitrix/components/bitrix/blog/templates/general_page/bitrix/blog.popular_blogs/.default/lang/
bitrix/components/bitrix/blog/templates/general_page/bitrix/blog.popular_blogs/.default/lang/en/
bitrix/components/bitrix/blog/templates/general_page/bitrix/blog.popular_blogs/.default/lang/en/.parameters.php
bitrix/components/bitrix/blog/templates/general_page/bitrix/blog.popular_blogs/.default/lang/ru/
bitrix/components/bitrix/blog/templates/general_page/bitrix/blog.popular_blogs/.default/lang/ru/.parameters.php
bitrix/components/bitrix/blog/templates/general_page/bitrix/blog.popular_blogs/.default/template.php
bitrix/components/bitrix/blog/templates/general_page/bitrix/blog.popular_blogs/.default/.parameters.php
bitrix/components/bitrix/blog/templates/general_page/bitrix/blog.groups/
bitrix/components/bitrix/blog/templates/general_page/bitrix/blog.groups/.default/
bitrix/components/bitrix/blog/templates/general_page/bitrix/blog.groups/.default/template.php
bitrix/components/bitrix/blog/templates/general_page/bitrix/blog.new_blogs/
bitrix/components/bitrix/blog/templates/general_page/bitrix/blog.new_blogs/.default/
bitrix/components/bitrix/blog/templates/general_page/bitrix/blog.new_blogs/.default/lang/
bitrix/components/bitrix/blog/templates/general_page/bitrix/blog.new_blogs/.default/lang/en/
bitrix/components/bitrix/blog/templates/general_page/bitrix/blog.new_blogs/.default/lang/en/.parameters.php
bitrix/components/bitrix/blog/templates/general_page/bitrix/blog.new_blogs/.default/lang/ru/
bitrix/components/bitrix/blog/templates/general_page/bitrix/blog.new_blogs/.default/lang/ru/.parameters.php
bitrix/components/bitrix/blog/templates/general_page/bitrix/blog.new_blogs/.default/template.php
```

Рис. 6: Процесс восстановления бэкапа

GitLab RCE. Заходим на панель администратора, ужесточаем регистрацию (рис. [-@fig:005])

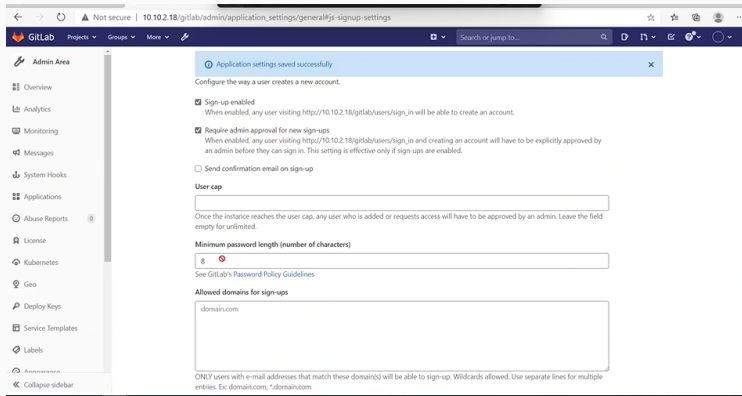


Рис. 7: Настройки регистрации

GitLab RCE. Удаляем неизвестного нам пользователя (рис. [-@fig:006])

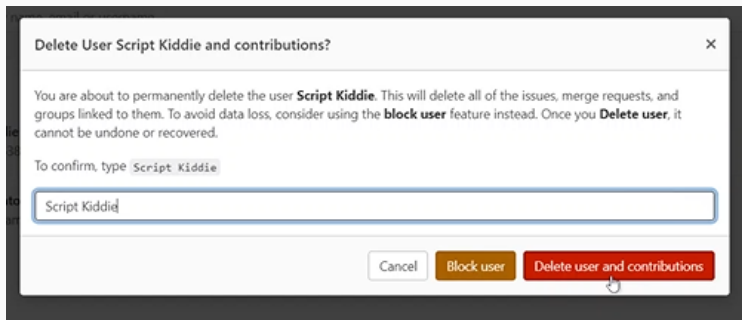


Рис. 8: Удаляем неизвестного нам пользователя

GitLab RCE. Находим PID сессию с нарушителем, убиваем её (рис. [-@fig:007])

```
users:({"prometheus",pid=18712,fd=21))
ESTAB  0      0      127.0.0.1:9187      127.0.0.1:40744
users:({"postgres_export",pid=18586,fd=7))
ESTAB  0      0      127.0.0.1:9229      127.0.0.1:41366
users:({"gitlab-workhors",pid=18535,fd=10))
ESTAB  0      0      127.0.0.1:9100      127.0.0.1:48432
users:({"node_exporter",pid=18580,fd=7))
root@ampire-gitlab:/home# kill -9 4263
root@ampire-gitlab:/home#
```

Рис. 9: Сессия нарушителя устранена

WSO2 API-Manager RCE. Заходим на MS API Manager, изменяем параметр загрузки ресурсов (рис. [-@fig:008])

```
[[resource.access_control]]
context = "(.*)/fileupload/(.*)"
secure=true
http_method="all"
permissions=["/permission/protected/"]
```

Рис. 10: Меняем конф

WSO2 API-Manager RCE. Удаляем бэкдор (рис. [-@fig:009])

```
users: (("payload.elf",pid=4792,fd=3))
root@wso2-virtual-machine:/home/user# nano /opt/wso2am-4.0.0/re
release-notes.html repository/ resources/
root@wso2-virtual-machine:/home/user# nano /opt/wso2am-4.0.0/repository/conf/dep
loyment.toml
root@wso2-virtual-machine:/home/user# cd /tmp
root@wso2-virtual-machine:/tmp# rm payload.elf
root@wso2-virtual-machine:/tmp# cd /opt/wso2am-4.0.0/repository/deployment/serve
r/webapps/authenticationendpoint/
root@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/deployment/server/webapps
/authenticationendpoint# rm exploit.jsp
root@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/deployment/server/webapps
/authenticationendpoint#
```

Рис. 11: Удалили бэкдор

WSO2 API-Manager RCE. Удаляем нового пользователя (рис. [-@fig:009])

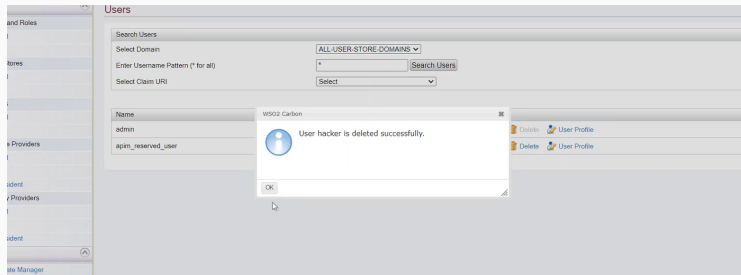


Рис. 12: Удалили бэкдор

Все атаки и их последствия успешно устранены

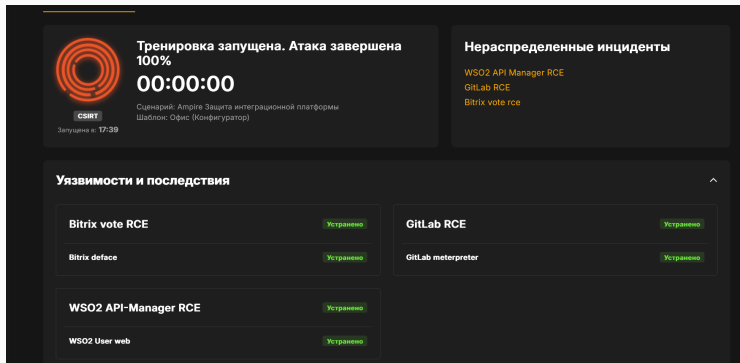


Рис. 13: Всё оки

Выводы

Отработали сценарий: Защита интеграционной платформы.