

Отчёт по лабораторной работе 3-D (НФИ-2)

**Программный комплекс обучения методам обнаружения,
анализа и устранения последствий компьютерных атак
«Ampire»**

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

Содержание

Цель работы	5
Задание	6
Выполнение лабораторной работы	7
Выводы	13
Список литературы	14

Список иллюстраций

1	Атакованные ip-адреса	7
2	Карточка инцидента “Bitrix vote RCE”	8
3	Карточка инцидента “GitLab RCE”	8
4	Добавили карточку инцидента “WSO2 API-Manager RCE”	9
5	.htaccess	9
6	Процесс восстановления бэкапа	10
7	Настройки регистрации	10
8	Удаляем неизвестного нам пользователя	11
9	Сессия нарушителя устранена	11
10	Меняем конф	11
11	Удалили бэкдор	12
12	Удалили бэкдор	12
13	Всё оки	12

Список таблиц

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

Выполнение лабораторной работы

На сайте ViPNet IDS NS просмотрели атакованные активы и суть атак (рис. [-@fig:002])

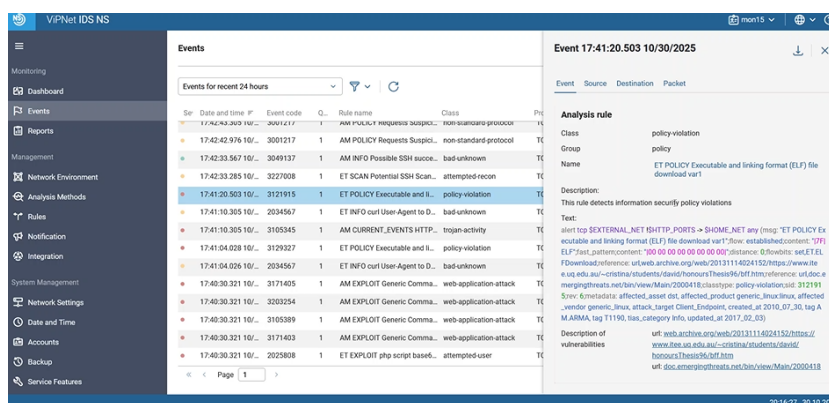


Рис. 1: Атакованные ip-адреса

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)

Поражённые активы

10.10.1.33 (Bitrix CMS)

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 эксплоиты

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

GitLab RCE

Дата и время события

30.10.2025 17:43

Источник

10.10.1.33 (Bitrix CMS)

Поражённые активы

10.10.2.18 (GitLab)

Описание

Workhorse передает файлы в библиотеку `ExifTool`, которая удаляет из них метаданные. Библиотека `ExifTool` различает файлы не по расширению, а по их контенту и подбирает соответствующий фильтр.

Рекомендации

2) активация функции подтверждения создания аккаунта администратором GitLab (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])

8

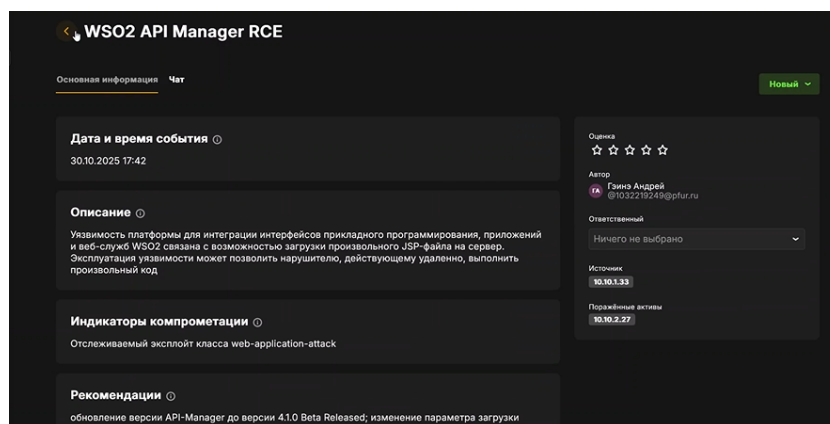


Рис. 4: Добавили карточку инцидента “WSO2 API-Manager RCE”

Bitrix vote RCE. Устранили уязвимость путём отклонения всех запросов к директории vote (рис. [-@fig:003])



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/temp
late.php
bitrix/components/bitrix/blog/templates/general_page/bitrix/blog.popular_blogs/.default/.par
ameters.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.ph
p
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])

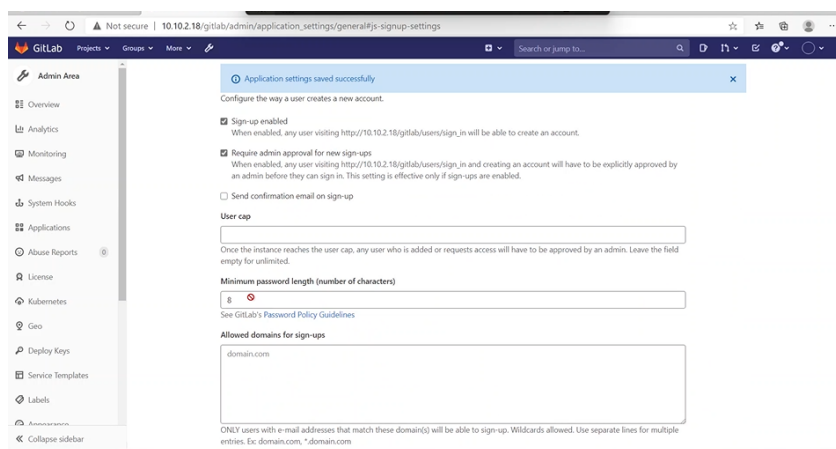


Рис. 7: Настройки регистрации

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

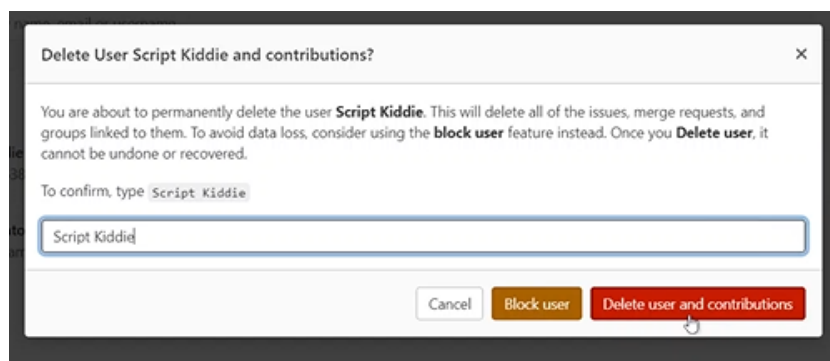


Рис. 8: Удаляем неизвестного нам пользователя

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])

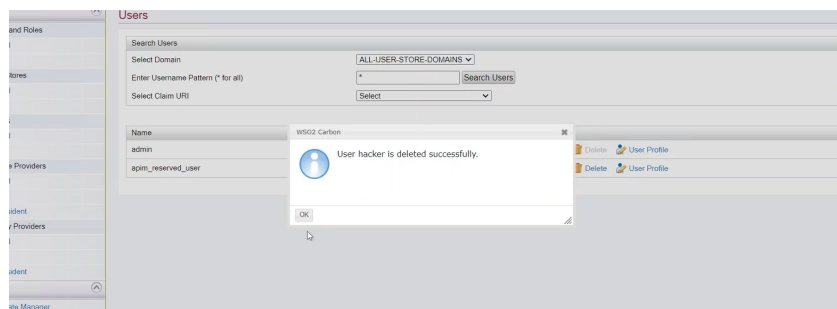


Рис. 12: Удалили бэкдор

Все атаки и их последствия успешно устранены

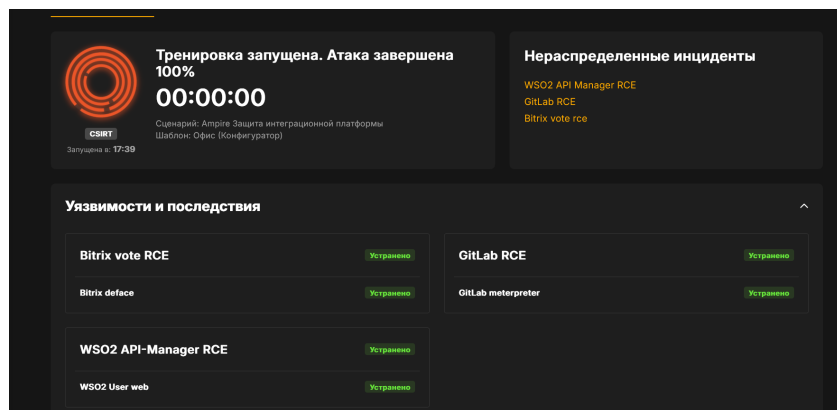


Рис. 13: Всё оки

Выводы

Отработали сценарий: Защита интеграционной платформы.

Список литературы

1. **CVE-2019-0630** — Common Vulnerabilities and Exposures.
URL: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0630>
2. **CVE-2019-17427** — Уязвимость XSS в Redmine.
URL: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17427>
3. **CVE-2019-18890** — Уязвимость Blind SQL-инъекции в Redmine.
URL: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-18890>