

# **Лабораторная работа №1**

**Кибербезопасность предприятия**

Аскеров Александр Эдуардович

Замбалова Дина Владимировна

Кузнецова София Вадимовна

Поляков Глеб Сергеевич

Скандарова Полина Юрьевна

Тарутина Кристина Еленовна

Цвелев Сергей Андреевич

Шулужук Айраана Вячеславовна

Учебная группа: НПИбд-01-22

# Содержание

<b>Цель работы</b>	<b>5</b>
<b>Теоретическое введение</b>	<b>6</b>
Легенда. Защита корпоративного мессенджера . . . . .	6
Описание уязвимостей . . . . .	6
WpDiscuz . . . . .	6
Proxylogon . . . . .	7
RocketChat . . . . .	7
<b>Выполнение лабораторной работы</b>	<b>8</b>
Уязвимый узел WpDiscuz . . . . .	9
Обнаружение уязвимости . . . . .	9
Обнаружение и нейтрализация полезных нагрузок. . . . .	10
Уязвимый узел Proxylogon . . . . .	18
Обнаружение CVE 2021-26855 (SSRF) средствами ОС . . . . .	19
Обнаружение CVE 2021-26855 (SSRF) средствами ViPNet IDS NS . .	20
Устранение уязвимостей . . . . .	22
Уязвимый узел RocketChat . . . . .	24
Обнаружение CVE-2021-22911 (NoSQL Injection) . . . . .	26
Устранение CVE-2021-22911 (NoSQL Injection) . . . . .	26
Обнаружение и нейтрализация полезных нагрузок . . . . .	30
Карточки инцидентов . . . . .	31
<b>Вывод</b>	<b>33</b>
<b>Список литературы</b>	<b>34</b>

# Список иллюстраций

1	Подключение к серверу . . . . .	8
2	Вектор атаки . . . . .	9
3	Подключение к удаленному рабочему столу . . . . .	11
4	Просмотр пароля . . . . .	11
5	Вход в KeyPass 2 . . . . .	12
6	Папка атакованного сервера . . . . .	12
7	Атакованный сервер . . . . .	13
8	Авторизация . . . . .	13
9	Плагин UpdraftPlus в репозитории WordPress . . . . .	14
10	Существующие резервные копии UpdraftPlus . . . . .	15
11	Компоненты для восстановления . . . . .	15
12	Ошибка восстановления . . . . .	16
13	Успешное выполнение восстановления . . . . .	16
14	Обновленная страница сайта . . . . .	17
15	Отображение информации о TCP-соединениях. Процесс закрытия meterpreter-сессии . . . . .	18
16	Уязвимость и последствия устранены . . . . .	18
17	Подключение к удаленному рабочему столу . . . . .	19
18	Подключение к удаленному рабочему столу . . . . .	19
19	Артефакты, оставленные атакой в журнале «IIS» . . . . .	20
20	Артефакты, оставленные атакой в журнале «IIS» . . . . .	20
21	Вход в ViPNet IDS NS . . . . .	21
22	Список событий, направленных на уязвимый сервер . . . . .	21
23	Окно Internet Information Services (IIS) Manager . . . . .	22
24	«IP Address and Domain Restrictions» . . . . .	22
25	Сокет с узлом нарушителя . . . . .	23
26	Завершение процессов . . . . .	23
27	Удаление файла . . . . .	24
28	Уязвимость и последствия устранены . . . . .	24
29	Восстановление пароля . . . . .	27
30	Ссылка для сброса пароля . . . . .	27
31	Генерация одноразового пароля . . . . .	28
32	Генерация одноразового пароля . . . . .	28
33	Двухфакторная аутентификация . . . . .	29
34	Настройка конфигурации БД . . . . .	29
35	Пример сокета с узлом нарушителя . . . . .	30
36	Уязвимость и последствия устранены . . . . .	30

37	WP Discuz RCE . . . . .	31
38	Proxylogon . . . . .	31
39	Rocketchat RCE . . . . .	32

# **Цель работы**

Целью лабораторной работы является исследование сценария целенаправленной атаки на корпоративный мессенджер и сопутствующие сервисы, выявить и продемонстрировать эксплуатацию реальных уязвимостей (WpDiscuz, ProxyLogon, RocketChat), а также отработать методы обнаружения, локализации и нейтрализации последствий компрометации для восстановления безопасности информационной инфраструктуры организации.

# **Теоретическое введение**

## **Легенда. Защита корпоративного мессенджера**

Конкуренты решили скомпрометировать деятельность Компании и нашли для этого исполнителя. Злоумышленник находит в Интернете сайт соответствующего предприятия и решает провести атаку на него с целью получения доступа к внутренним ресурсам. Проэксплуатировав обнаруженную на сайте уязвимость, нарушитель стремится захватить управление другими ресурсами защищаемой сети, в том числе, пытается закрепиться на почтовом сервере и продолжить атаку. Главная задача злоумышленника - получение доступа к переписке сотрудников компании, раскрытие учётных данных пользователей, зарегистрированных в приложении корпоративного мессенджера, с целью использования их для нанесения ущерба репутации конкурирующей Компании. Квалификация нарушителя высокая. Он умеет использовать инструментарий для проведения атак, а также знает техники постэксплуатации.

## **Описание уязвимостей**

### **WpDiscuz**

CVE-2020-24186 – это уязвимость в плагине для создания комментариев WpDiscuz версии с 7.0.0 по 7.0.4 включительно. Уязвимость позволяет получить RCE (удаленное выполнение кода).

## **Proxylogon**

Proxylogon представляет собой SSRF уязвимость, позволяющую обойти аутентификацию и выдать себя за администратора.

Следующий шаг после SSRF – эксплуатация CVE 2020-27065. Данная уязвимость является следствием неэффективного ограничения выбора расположения backup виртуальной директории автономных адресных книг.

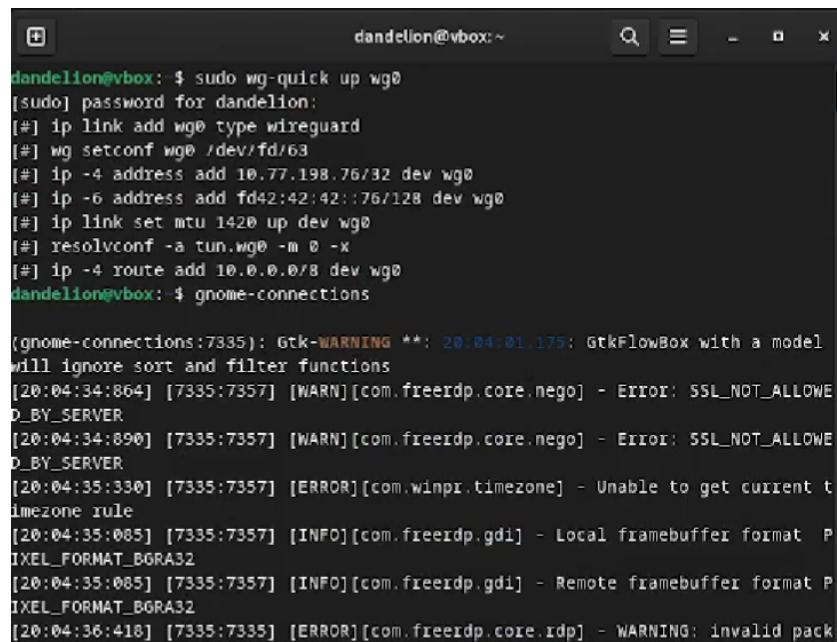
## **RocketChat**

CVE-2021-22911 представляет собой сочетание из двух SQL-инъекций: - следящая NoSQL-инъекция, - NoSQL-инъекция №2: повышение привилегий.

CVE-2022-0847 (Dirty Pipe) представляет собой уязвимость повышения привилегий, находящаяся в самом ядре Linux версии 5.8 и выше.

# Выполнение лабораторной работы

Подключили vpn WireGuard, чтобы открыть сайт Ampire с лабораторной работой (рис. 1).



```
dandelion@vbox: ~
dandelion@vbox: $ sudo wg-quick up wg0
[sudo] password for dandelion:
[#] ip link add wg0 type wireguard
[#] wg setconf wg0 /dev/fd/63
[#] ip -4 address add 10.77.198.76/32 dev wg0
[#] ip -6 address add fd42:42:42::76/128 dev wg0
[#] ip link set mtu 1420 up dev wg0
[#] resolvconf -a tun.wg0 -m 0 -x
[#] ip -4 route add 10.0.0.0/8 dev wg0
dandelion@vbox: $ gnome-connections

(gnome-connections:7335): Gtk-WARNING **: 20:04:01.175: GtkFlowBox with a model
will ignore sort and filter functions
[20:04:34:864] [7335:7357] [WARN][com.freerdp.core.nego] - Error: SSL_NOT_ALLOWE
D_BY_SERVER
[20:04:34:890] [7335:7357] [WARN][com.freerdp.core.nego] - Error: SSL_NOT_ALLOWE
D_BY_SERVER
[20:04:35:330] [7335:7357] [ERROR][com.winpr.timezone] - Unable to get current t
imezone rule
[20:04:35:085] [7335:7357] [INFO][com.freerdp.gdi] - Local framebuffer format P
IXEL_FORMAT_BGRA32
[20:04:35:085] [7335:7357] [INFO][com.freerdp.gdi] - Remote framebuffer format P
IXEL_FORMAT_BGRA32
[20:04:36:418] [7335:7335] [ERROR][com.freerdp.core.rdp] - WARNING: invalid pack
```

Рис. 1: Подключение к серверу

Рассмотрим вектор атаки (рис. 2).

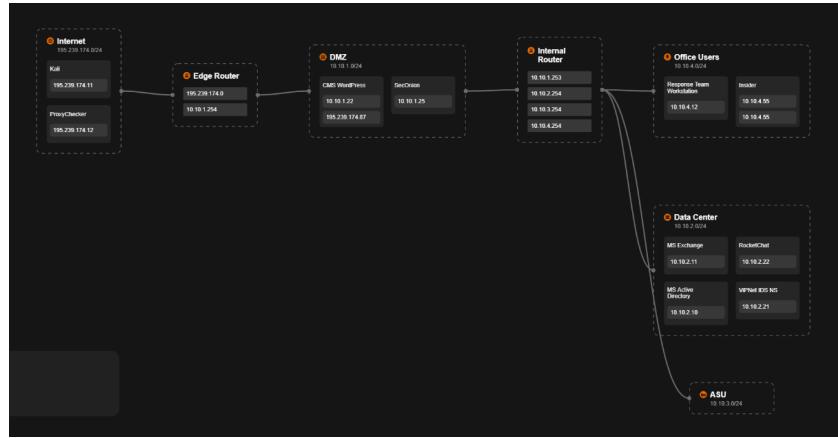


Рис. 2: Вектор атаки

## Уязвимый узел WpDiscuz

### Обнаружение уязвимости

Среди множества плагинов в CMS WordPress можно выделить WpDiscuz – один из плагинов для создания комментариев. WpDiscuz представляет собой систему для комментариев на базе Ajax, которая хранит сообщения в локальной базе данных. В версиях с 7.0.0 по 7.0.4 включительно существует уязвимость File Upload, которая позволяет получить RCE, если прикрепить любой файл (например, код на PHP) в поле для комментариев и загрузить на сервер. Данный процесс можно выполнить без аутентификации. Уязвимость позволяет получить удаленное выполнение кода при загрузке неавторизированным пользователем определенного файла с расширением PHP, достаточно прикрепить файл с PHP-кодом в поле для ввода комментариев [1].

После создания файла с полезной нагрузкой нарушитель будет производить POST-запрос с определенными параметрами по ссылке <http://webportal3.ampire.corp/index.php/admin/admin-ajax.php> для загрузки файла. Факт загрузки будет детектироваться в журнале активности в WordPress, в котором записывается хронологическая запись последовательности изменений и действий. В первую очередь необходимо

димо войти в панель администратора, для чего в адресной строке браузера <http://IP-адрес> дописать один из вариантов: - /wp-admin – на вход в панель управления; - /wp-login.php – вход на страницу регистрации

С помощью WP Activity Log можно проверить журнал и обнаружить время, дату, роль и IP-адрес пользователя, который внес изменения. По информации из журналов на сервере можно отыскать причину взлома и устранить возникшие уязвимости. Далее перейти в Activity Log, обнаружить авторизацию внешнего пользователя и загрузку файла. Из файла журнала сервера apache2, который находится по пути /var/log/apache2/access.log, можно отметить подозрительную активность, заключающуюся в множественных запросах к страницам авторизации, административному файлу admin-ajax.php, а также запросу на чтение файла readme.txt. В User-Agent присутствует pythonrequests/2.28.1, что может свидетельствовать об использовании скрипта на Python для выполнения запросов.

Детектирование эксплуатации уязвимости удаленного выполнения кода CVE-2020-24186 проводится с помощью сетевого сенсора ViPNet IDS NS.

## **Обнаружение и нейтрализация полезных нагрузок.**

Для начала скачали приложение Remmina, чтобы подключиться к удаленному рабочему столу. Запустили его, ввели указанный на сайте Ampire ip-адрес 10.140.2.180, ввели логин и пароль (рис. 3).

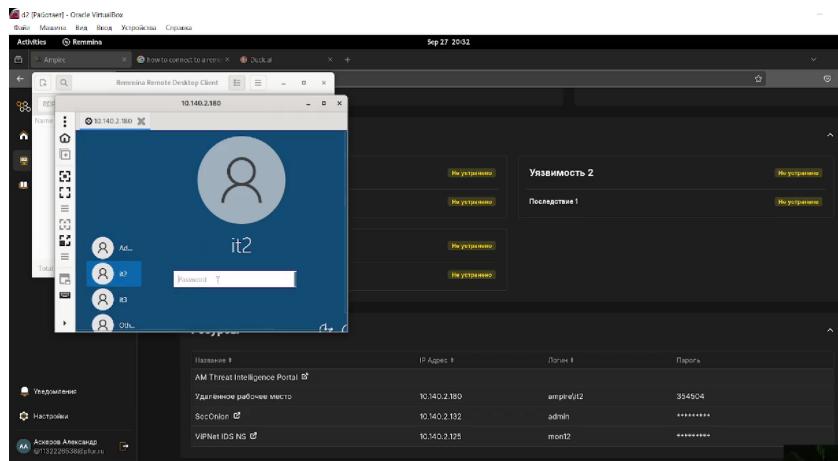


Рис. 3: Подключение к удаленному рабочему столу

В файле KeyPass password посмотрели пароль для KeyPass 2 (рис. 4).

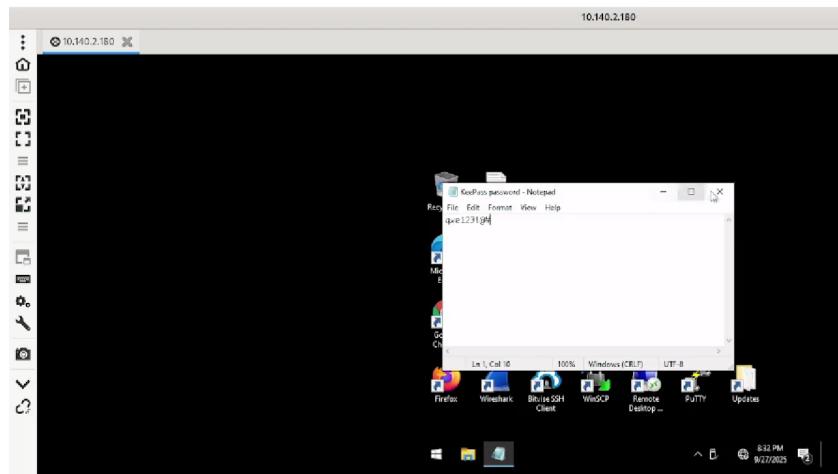


Рис. 4: Просмотр пароля

Заходим в KeyPass 2, вводим пароль (рис. 5).



Рис. 5: Вход в KeyPass 2

Так как у нас атакован сервер CMS WordPress, мы переходим в папку DMZ, затем в CMS WordPress (рис. 6).

Title	User Name	Protocol	URL
CMS WordPress WEB	admin	*****	http://10.10.1.2
CMS WordPress SSH via PuTTY	user	*****	http://10.10.1.22/xp-Login.php
CMS WordPress SSH via Bitvise	user	*****	ssh-bitvise://70
CMS WordPress SCP	user	*****	scp://10.10.1.22
CMS WordPress MySQL	admin_joe	*****	

Рис. 6: Папка атакованного сервера

Посмотрим на атакованный сайт 10.10.1.22 (<http://webportal3.ampire.corp>) (рис. 7).



Рис. 7: Атакованный сервер

Deface сайта. Данная полезная нагрузка подразумевает изменение интерфейса главной страницы сайта.

Чтобы войти в панель администратора, зайдем на страницу регистрации <http://10.10.1.22/wp-login.php>. Логин и пароль берем из KeyPass 2 (рис. 8).

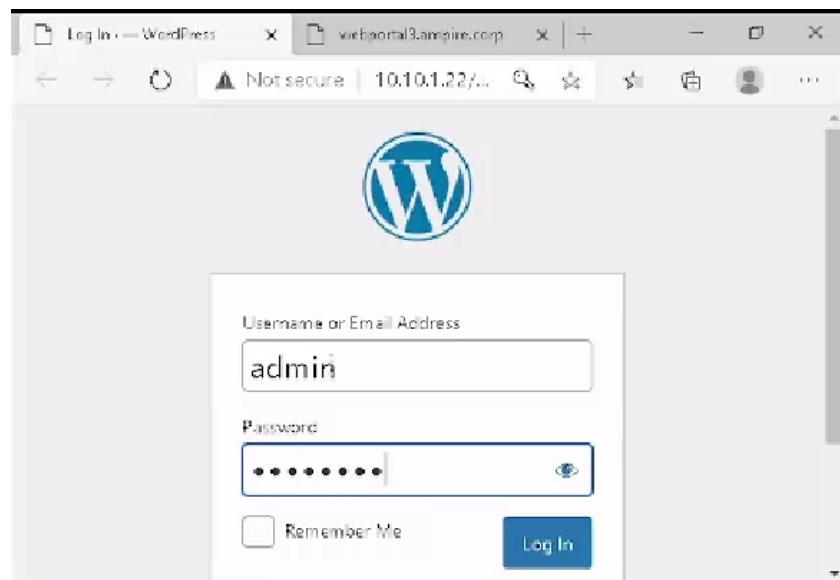


Рис. 8: Авторизация

Deface сайта. Данная полезная нагрузка подразумевает изменение интерфейса главной страницы сайта.

са главной страницы сайта.

Закрытие полезной нагрузки: на веб-сервере работает FTP-сервер vsftpd, который дает возможность плагину i сохранять и скачивать резервную копию. Таким образом, можно выполнить восстановление из последнего файла резервной копии.

Для нейтрализации данной полезной нагрузки необходимо сформировать резервную копию с помощью плагина Updraft Backup/Restore. Этапы восстановления: - в панели управления на странице Plugins найти плагин резервного восстановления UpdraftPlus, открыть настройки (рис. 9)

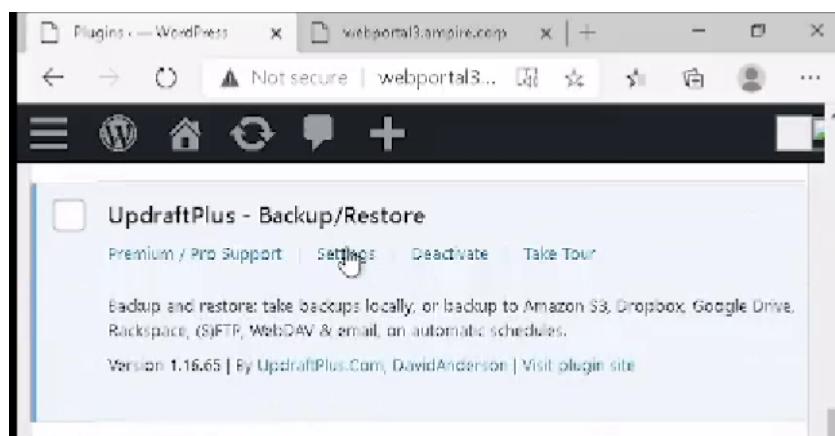


Рис. 9: Плагин UpdraftPlus в репозитории WordPress

- для восстановления нажать Restore на последней резервной копии (рис. 10)

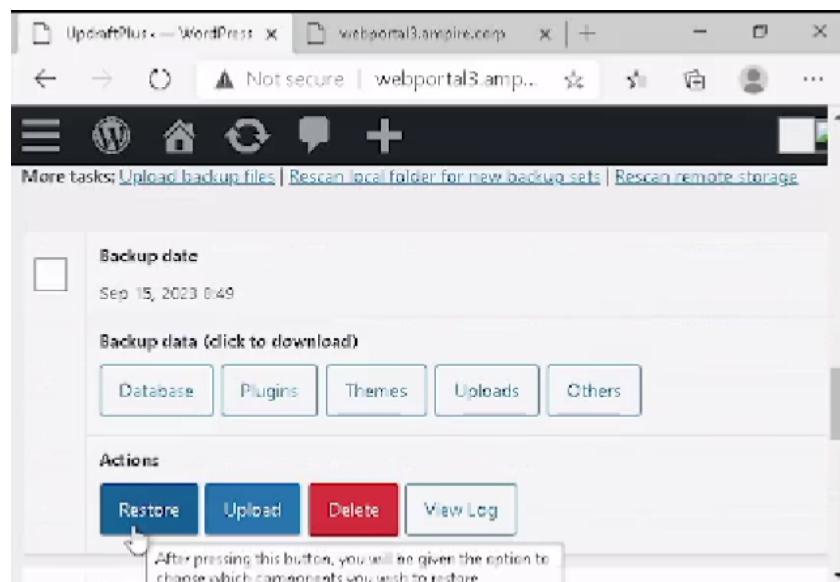


Рис. 10: Существующие резервные копии UpdraftPlus

- далее в выпадающем окне выбора компонентов для восстановления выбрать только Themes и Uploads (рис. 11)

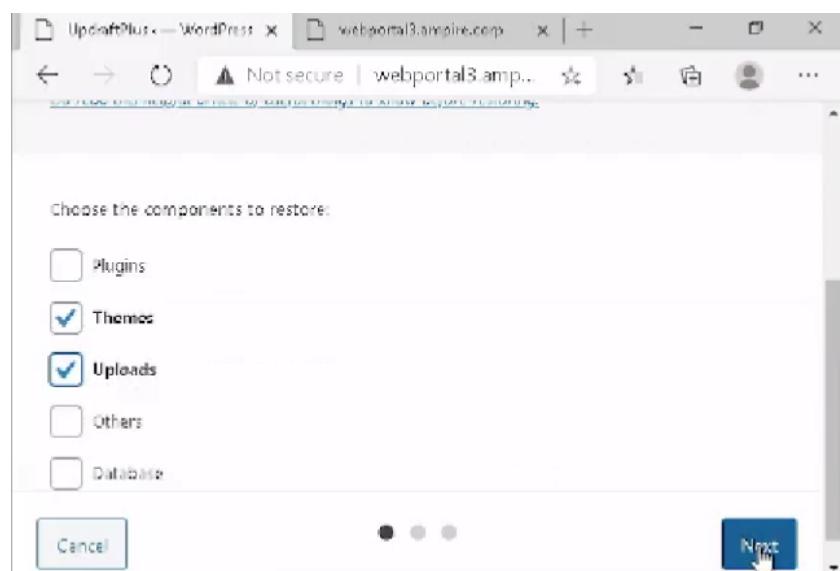


Рис. 11: Компоненты для восстановления

- далее нажать Next и Restore;
- при возникновении ошибки необходимо в журнале действий нажать на опцию Delete Old Directories (рис. 12)

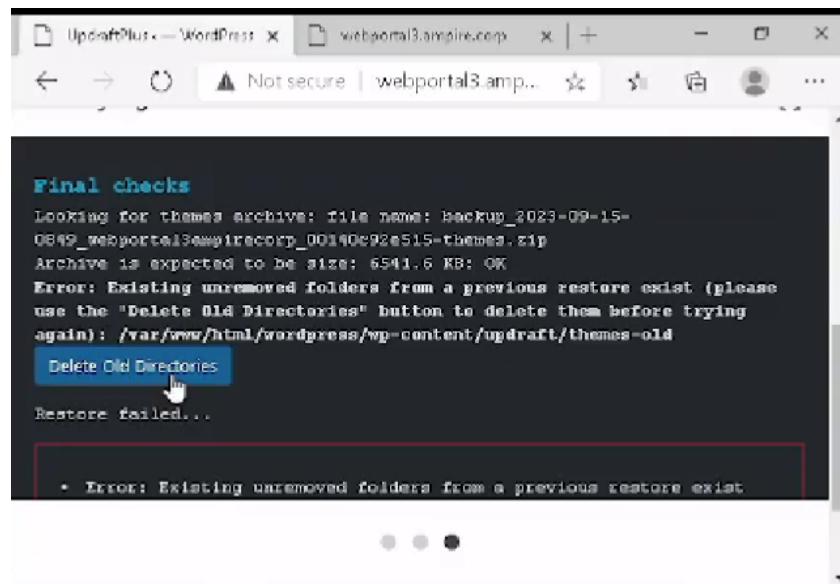


Рис. 12: Ошибка восстановления

- осуществить возврат к конфигурации, активировать опцию Return to configuration (рис. 13)

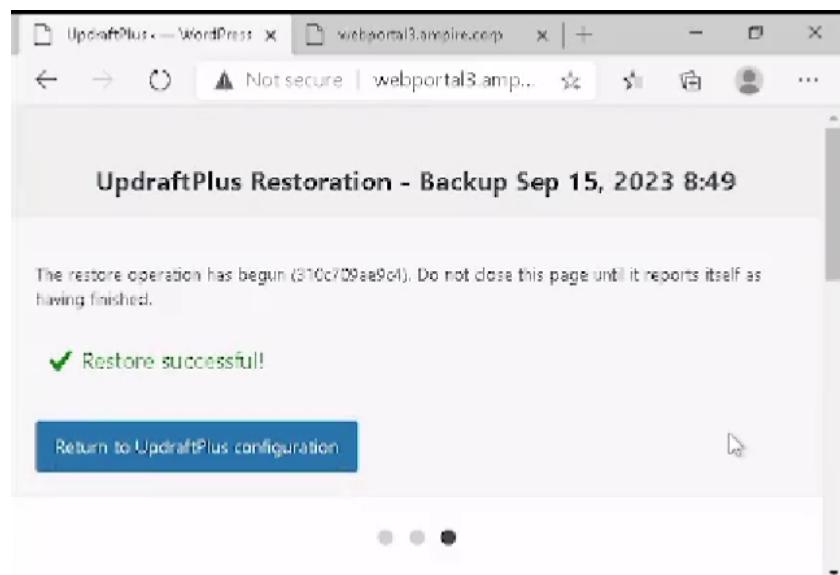


Рис. 13: Успешное выполнение восстановления

После обновления страницы откроется первоначальная картинка сайта (рис. 14)

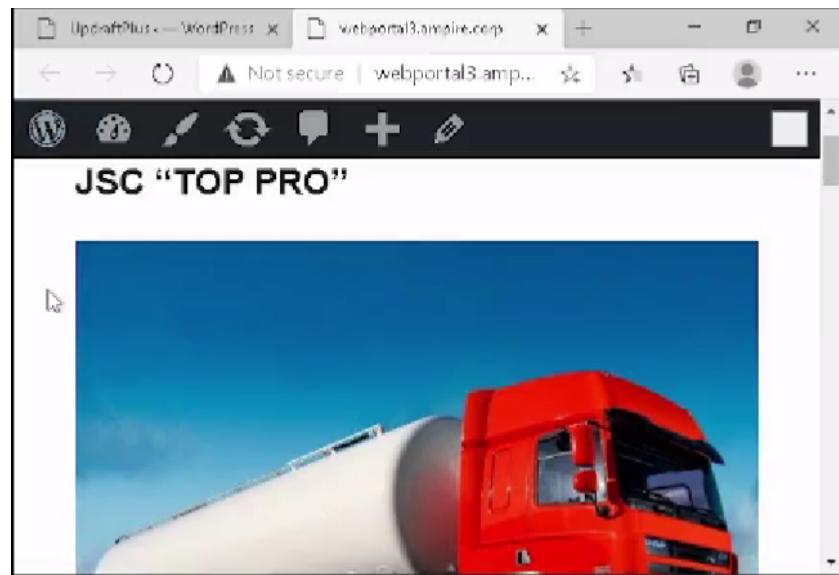


Рис. 14: Обновленная страница сайта

Последствие успешно устранено.

**Meterpreter-сессия.** Данная полезная нагрузка заключается в том, что нарушитель устанавливает shell-сессию с уязвимой машиной. Для обнаружения meterpreter-сессии необходимо проверить сокеты уязвимой машины на подключение к определенному порту машины нарушителя с помощью утилиты ss. Просмотреть сокеты только нужного протокола TCP и отфильтровать данные (например, вывести только активные TCP-соединения) можно с помощью команды: ss -tnp

Для закрытия вредоносного сокета необходимо завершить процесс, использующийся для поддержания соединения. При завершении процесса определить уникальный идентификатор процесса (PID) и прописать команду kill с соответствующими параметрами (рис. 15).

```

user@web-portal-3:~$ sudo ss -tp
State      Recv-Q Send-Q Local Address:Port          Peer Address:Port
CLOSE_WAIT  0        0      10.10.1.22:39654       195.239.174.11:5557   users:({"chisel.sh",pid=1923,fd=12}, {"sh",pid=1922,fd=12}, {"KLoWi",pid=1089,fd=12})
FIN_WAIT_2  0        0      10.10.1.22:55518       10.10.2.11:443    users:({"chisel.sh",pid=1923,fd=16})
ESTAB     0        0      10.10.1.22:55396       195.239.174.11:5556   users:({"chisel.sh",pid=1923,fd=3}, {"sh",pid=1922,fd=3}, {"KLoWi",pid=1089,fd=3})
ESTAB     0        0      10.10.1.22:48992       195.239.174.11:1085   users:({"chisel.sh",pid=1923,fd=11})
ESTAB     0        64     10.10.1.22:22227       10.10.1.23:59706   users:({"sshd",pid=10666,fd=3}, {"sshd",pid=10545,fd=3})
user@web-portal-3:~$ kill 1889
-bash: kill: (1889) - Operation not permitted
user@web-portal-3:~$ sudo ss -tp4
State      Recv-Q Send-Q Local Address:Port          Peer Address:Port
CLOSE_WAIT  0        0      10.10.1.22:39654       195.239.174.11:5557   users:({"chisel.sh",pid=1923,fd=12}, {"sh",pid=1922,fd=12})
FIN_WAIT_2  0        0      10.10.1.22:55518       10.10.2.11:https   users:({"chisel.sh",pid=1923,fd=16})
ESTAB     0        0      10.10.1.22:53386       195.239.174.11:freeciv  users:({"chisel.sh",pid=1923,fd=3}, {"sh",pid=1922,fd=3})
ESTAB     0        0      10.10.1.22:55502       195.239.174.11:5556   users:({"chisel.sh",pid=1923,fd=16})
ESTAB     0        64     10.10.1.22:8888       10.10.1.23:51756   users:({"sshd",pid=10666,fd=3}, {"sshd",pid=10545,fd=3})
user@web-portal-3:~$ sudo kill 1923
user@web-portal-3:~$ sudo ss -tp4
State      Recv-Q Send-Q Local Address:Port          Peer Address:Port
CLOSE_WAIT  0        0      10.10.1.22:39654       195.239.174.11:5557   users:({"chisel.sh",pid=1923,fd=12})
LAST_ACK   0        1      10.10.1.22:55518       10.10.2.11:https   users:({"chisel.sh",pid=1923,fd=16})
FIN_WAIT_2  0        0      10.10.1.22:55502       10.10.1.22:sshd   users:({"chisel.sh",pid=1923,fd=3})
ESTAB     0        64     10.10.1.22:22227       10.10.1.23:59706   users:({"sshd",pid=10666,fd=3}, {"sshd",pid=10545,fd=3})
users:({"sshd",pid=10666,fd=3}, {"sshd",pid=10545,fd=3})

```

Рис. 15: Отображение информации о TCP-соединениях. Процесс закрытия meterpreter-сессии

Уязвимость и последствия WpDiscuz устраниены (рис. 16).

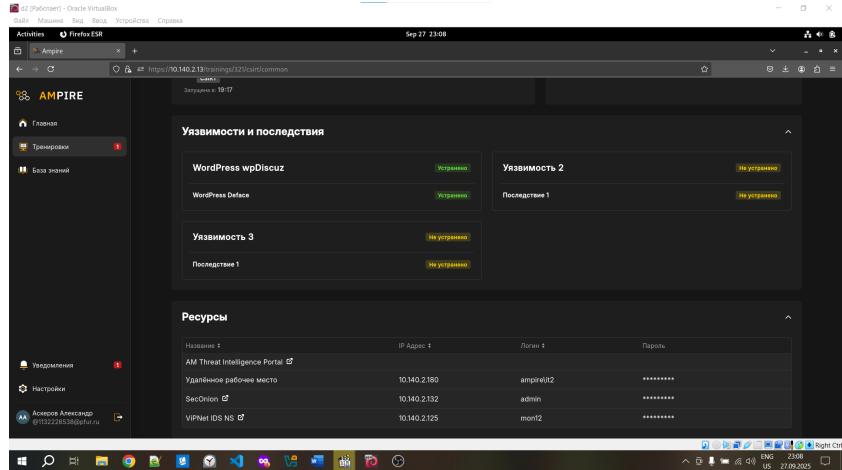


Рис. 16: Уязвимость и последствия устраниены

## Уязвимый узел Proxylogon

Подделка запроса на стороне сервера – это атака, которая позволяет отправлять запросы от имени сервера к внешним или внутренним ресурсам. Нарушитель может контролировать весь запрос целиком или отдельные части запроса (например, домен). Для эксплуатации уязвимости SSRF должно быть выполнено три условия: - нарушитель должен знать один работающий e-mail; - раздел cookie «X-BEResource» должен содержать FQDN атакуемого сервера + /autodiscover/autodiscover.xml?a=~1. Значение cookie обязательно должно заканчиваться на цифру; - тело запроса содержит специально сформированный XML

SOAP [2].

## Обнаружение CVE 2021-26855 (SSRF) средствами ОС

Снова подключились к удаленному рабочему столу с ip-адресом 10.140.2.153 (рис. 17).

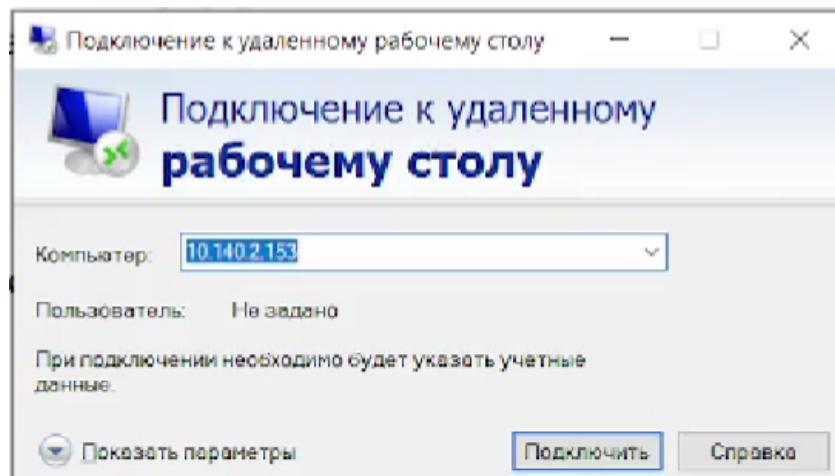


Рис. 17: Подключение к удаленному рабочему столу

Внутри него подключились к удаленному рабочему столу с ip-адресом атакованного сервера 10.10.2.11 (рис. 18).

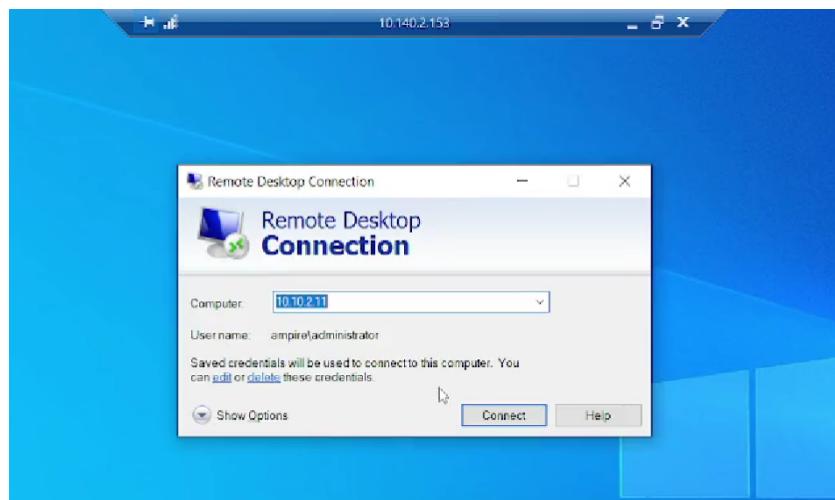


Рис. 18: Подключение к удаленному рабочему столу

Все запросы, подробно представленные в соответствующем описании, могут быть обнаружены в логах IIS. Логи расположены в директории C:/inetpub/logs/LogFiles. В логах необходимо перейти в папку атакуемого сервера (W3SVC1) и в данной папке просмотреть новый файл. Примеры возможных логов атаки изображены на скриншотах (рис. 19-20).

Рис. 20: Артефакты, оставленные атакой в журнале «IIS»

В скрипте обнаружены запросы, где нарушитель получает SID искомого пользователя с помощью HTTP-запроса к MAPI. Нарушитель отправляет запрос для делегирования доступа к почтовому ящику. Данный запрос также перенаправляется к MAPI от имени пользователя машинного аккаунта и вызывает ошибку доступа. Ошибка содержит SID искомого пользователя, после получения которого нарушитель сможет аутентифицироваться на сервере. Нарушитель выдает себя за администратора, отправляет на /ecp/proxyLogon.ecp POST запрос, сформированный специальным образом.

## Обнаружение CVE 2021-26855 (SSRF) средствами ViPNet IDS NS

С удаленного рабочего стола авторизуемся в ViPNet IDS NS. В фильтре укажем дату и время запуска лабораторной работы (рис. 21).

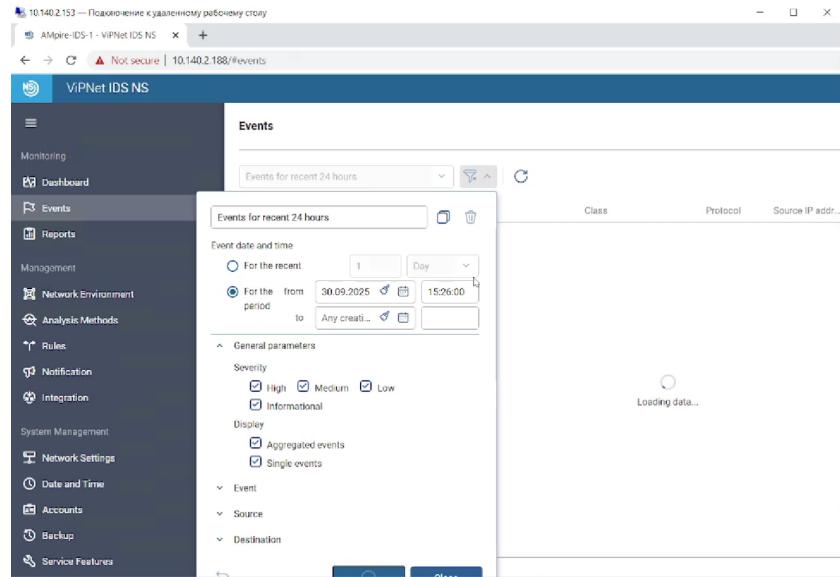


Рис. 21: Вход в ViPNet IDS NS

Proxylogon представляет собой SSRF в Exchange Server, позволяющую обойти аутентификацию и выдать себя за администратора. В сценарии данная уязвимость используется в связке с CVE 2021-27065 (запись файла в произвольную директорию). Уязвимости Proxylogon подвержены все Exchange Server 2016, до версии 15.01.2106.013. Сетевой сенсор ViPNet IDS NS во время атаки детектирует несколько событий, которые потенциально могут быть связаны с эксплуатацией уязвимости на уязвимом хосте (рис. 22).

● 15:29:16.558 09/...	2025644	1	ET TROJAN Possible Metasp...	trojan activity	TCP	195.239.174.11
● 15:29:16.557 09/...	2025644	1	ET TROJAN Possible Metasp...	trojan-activity	TCP	195.239.174.11
● 15:29:16.555 09/...	2035480	1	ET INFO PE EXE Download o...	misc-activity	TCP	195.239.174.11
● 15:29:16.555 09/...	2035480	1	ET INFO PE EXE Download o...	misc-activity	TCP	195.239.174.11

Рис. 22: Список событий, направленных на уязвимый сервер

В списке событий присутствуют признаки загрузки на уязвимый хост подозрительных файлов в формате .exe, событие № 1. Также зафиксирована активность вредоносного программного обеспечения Metasploit, событие № 2.

## Устранение уязвимостей

Во время эксплуатации уязвимости Proxylogon нарушитель совершает GET и POST запросы к /ecp. Достаточно ограничить доступ к указанной директории для запрета эксплуатации уязвимости. 1. Для открытия Internet Information Services (IIS) Manager необходимо нажать сочетание клавиш Win + R и в появившемся окне ввести inetmgr и нажать Enter. 2. В открывшемся окне перейти во вкладку MAIL/Sites/Default Web Site/ecp и нажать на IP Address and Domain Restrictions (рис. 23).

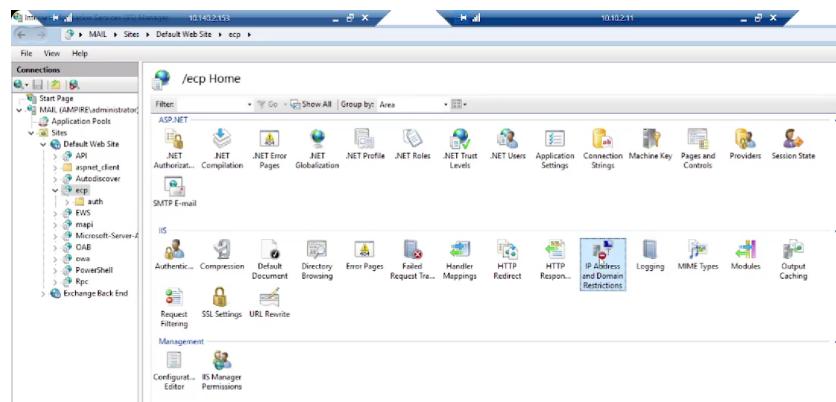


Рис. 23: Окно Internet Information Services (IIS) Manager

3. Далее в «Edit Feature Settings» – «Access for unspecified clients» выбрать пункт «Deny» и нажать «OK» (рис. 24).

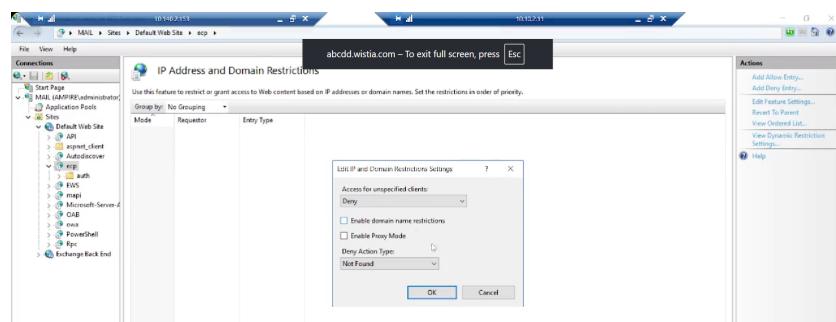


Рис. 24: «IP Address and Domain Restrictions»

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

Обнаружение и нейтрализация полезных нагрузок. Meterpreter-сессия. Данная полезная нагрузка заключается в получении нарушителем meterpreter-сессии с уязвимым сервером. Данную полезную нагрузку можно обнаружить с помощью утилиты netstat с ключами -b -o. В случае установления соединения на уязвимой машине появится сокет с машиной нарушителя (рис. 25).

TCP	10.10.2.11:7206	195.239.174.11:5558	ESTABLISHED	4260	
[powershell.exe]	TCP	10.10.2.11:7207	195.239.174.11:5558	ESTABLISHED	13136

Рис. 25: Сокет с узлом нарушителя

Для закрытия meterpreter-сессии необходимо завершить процесс данного соединения с помощью команды taskkill /PID /F. Данная команда в системе Windows используется для принудительного завершения процесса. На вход команда taskkill получает идентификатор процесса PID и параметр команды /F, который указывает на принудительное завершение процесса (рис. 26).

```
C:\Users\administrator.AMPIRE>taskkill /PID 4260 /F
SUCCESS: The process with PID 4260 has been terminated.

C:\Users\administrator.AMPIRE>taskkill /PID 13136 /F
SUCCESS: The process with PID 13136 has been terminated.

C:\Users\administrator.AMPIRE>
```

Рис. 26: Завершение процессов

Web-shell China Chopper. Backdoor «China Chopper» можно найти в очевидной для таких атак директории C:/Program Files/Microsoft/Exchange Server/V15/FrontEnd/HttpProxy/owa/auth/AM\_backdoor.aspx. Большинство РОС (проверок концепций) эксплуатации уязвимости Proxylogon записывают файл именно по данному адресу, что выполняется для доступа backdoor без авторизации из веб-директории owa/auth. При необходимости полезную нагрузку можно записать в другую директорию. В журнал «IIS» также попадает POST запрос к указанному backdoor. Для устранения полезной нагрузки необходимо: - удалить файл веб-оболочки по пути C:/Program Files/Microsoft/Exchange Server/V15/FrontEnd/HttpProxy/..auth/ (рис. 27)

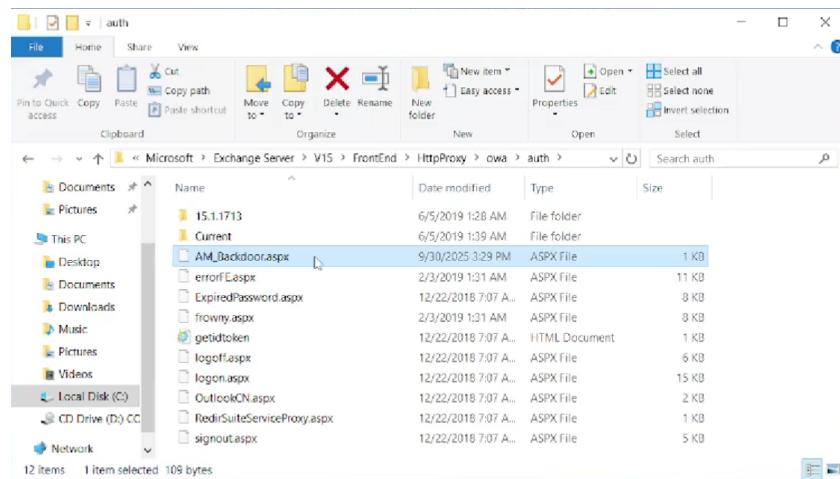


Рис. 27: Удаление файла

- завершить все соединения между уязвимой машиной и нарушителем.

Уязвимость и последствия Proxylogon устраниены (рис. 28).

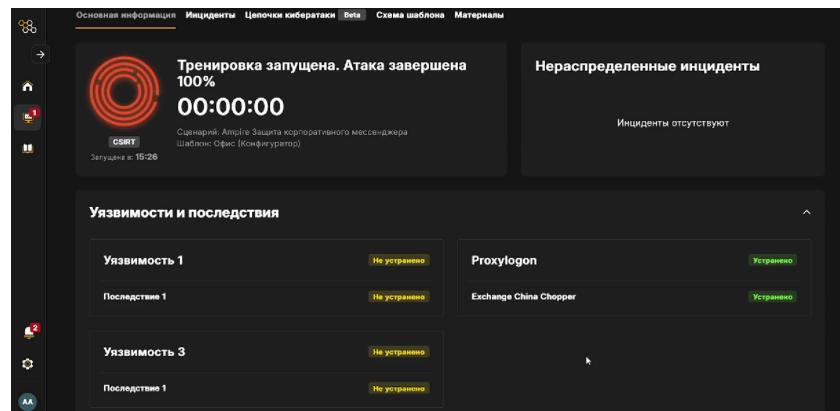


Рис. 28: Уязвимость и последствия устраниены

## Уязвимый узел RocketChat

CVE-2021-22911 представляет собой две уязвимости NoSQL Injection, эксплуатация которых может позволить злоумышленникам повысить свои привилегии, выполнить произвольные системные команды на хост-сервере и украсть конфиденциальные пользовательские данные и сообщения чата. Первая уязвимость CVE-2021-22911: слепая NoSQL-инъекция, позволяющая

украсть токен сброса пароля пользователя. Эксплуатация этой уязвимости работает следующим образом: злоумышленник запрашивает сброс пароля для пользователя, используя его адрес электронной почты. Далее использует уязвимость недостаточной проверки параметров запроса в методе getPasswordPolicy (server/methods/getPasswordPolicy.js), подставляет вместо токена-строки оператор БД regex с якорем ^, анализируя ответ сервера подбирает токен сброса пароля (находит первый символ, затем первые два и т.д.). №2: повышение привилегий. Данная уязвимость требует аутентификации, но имеет большее влияние: ее можно использовать не только для утечки токена сброса пароля пользователя, но и любого поля любого пользователя в базе данных. Конечная точка API users.list (app/api/server/v1/users.js) принимает параметр запроса из URL-адреса, который затем используется для запроса коллекции пользователей. Документы в этой коллекции содержат поля, которые не должны быть доступны всем, поэтому запрос фильтруется с помощью черного списка, который удаляет определенные поля из запроса и результата. Чтобы обойти фильтр, можно использовать оператор верхнего уровня where, который берет выражение JavaScript и выполняет его для каждого документа в коллекции, чтобы решить, должен ли документ содержаться в наборе результатов или нет. Для вывода информации используется выброс исключения с нужным полем: {"where": "this.username==='admin' && ()=>{ throw this.secret }()} Для достижения RCE злоумышленник может использовать встроенный в Rocket Chat механизм «Интеграции», который позволяет создавать входящие и исходящие webhook. Webhook могут иметь связанные с ними сценарии, которые выполняются при их срабатывании. На данном узле используется только вторая инъекция, так как подбор токена занимает много времени (около 30 минут), получение непrivилегированной учетной записи осуществляется путем регистрации нового аккаунта [3].

## **Обнаружение CVE-2021-22911 (NoSQL Injection)**

Эксплуатация первой инъекции сопровождается большим количеством запросов к серверу, так как идет подбор токена для смены пароля непривилегированного пользователя. Данное событие можно обнаружить в логах Rocket Chat из-за большого количества сообщений об ошибках в методе getPasswordPolicy.

Первая деталь эксплуатации второй NoSQL-инъекции - это невозможность осуществления входа на веб-интерфейс под учетными данными администратора (логин: admin@rocket-local.com, пароль: qwe123!@#). В syslog пишутся следующие строчки: - ошибка отправки приветственного сообщения при регистрации нового аккаунта; - письмо для сброса пароля админа; - ошибки при выполнении сценариев WebHook.

Также лог RocketChat доступен в веб-интерфейсе: «Администрирование» - «Просмотр логов». После восстановления пароля администратора в веб-интерфейсе RocketChat во вкладке «Администрирование» - «Интеграции» можно увидеть добавленные сценарии, зайдя в которые можно посмотреть выполненные команды.

Непосредственно эксплуатацию уязвимости обнаружить при помощи сетевого сенсора ViPNet IDS NS не получится, однако успешно детектируются последствия, а именно скачивание вредоносного файла для установки обратного TCP-соединения (meterpreter-сессии), и непосредственно установка этого соединения на 4444 порту.

## **Устранение CVE-2021-22911 (NoSQL Injection)**

Закрытие уязвимостей в Rocket Chat. Перейдем на удаленный рабочий стол.

Для восстановления доступа к аккаунту администратора необходимо сбросить пароль (рис. 29). Письмо с инструкциями для сброса пароля можно прочитать при помощи текстового редактора, прочитав файл /var/mail/admin.

Необходимо скопировать ссылку из письма, в данном примере (рис. 30).

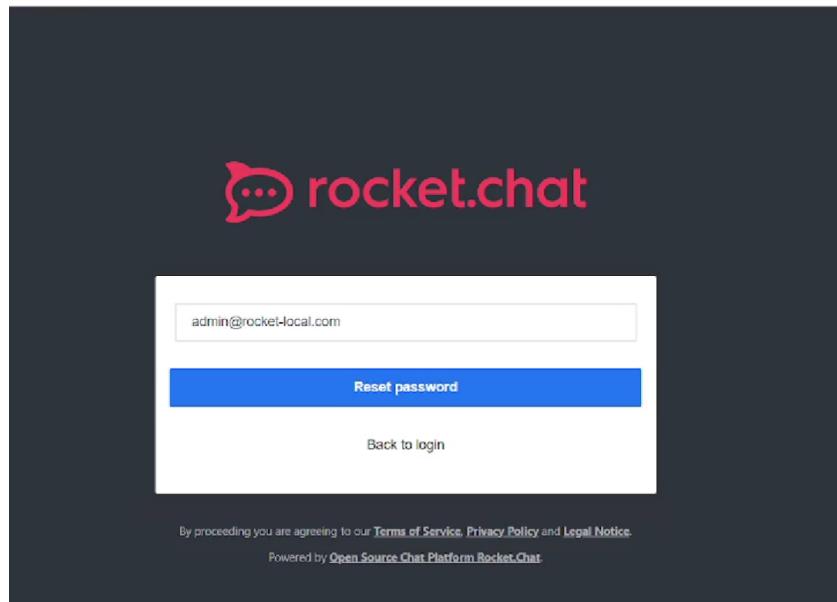


Рис. 29: Восстановление пароля

```
✉ admin@rocket-chat-server: /var/mail
Content-Type: multipart/alternative;
boundary="--_NmP-e16828c7e092e214-Part_1"
From: "Rocket.Chat" <rocketchat@rocket-local.com>
To: admin@rocket-local.com
Subject: Rocket.Chat - Password Recovery
Message-ID: <732d54fd-2fea-beef-b912-60a3523778b9@rocket-local.com>
Date: Tue, 30 Sep 2025 12:30:11 +0000
MIME-Version: 1.0

-----_NmP-e16828c7e092e214-Part_1
Content-Type: text/plain
Content-Transfer-Encoding: quoted-printable

Hello,

To reset your password, simply click the link below.

http://10.10.2.22:3000/reset-password/RW1X8ElterXd3Yc-PwBicaDrDnhRAunutMpAlv=1\_GD0j

Thanks.

-----_NmP-e16828c7e092e214-Part_1
Content-Type: text/html; charset=utf-8
```

Рис. 30: Ссылка для сброса пароля

Нужно обратить внимание, что в терминале при переносе строки используется знак «==», его следует игнорировать. После этого необходимо ввести новый пароль. Для учетной записи администратора Rocket Chat настроена двухфакторная аутентификация при помощи TOTP (Time-based one-time password).

Для генерации одноразового пароля необходимо воспользоваться программой KeePass, доступной на машине администрирования. В контекстном меню выбрать «KeeOtp2» - «Show TOTP» (рис. 31-32).

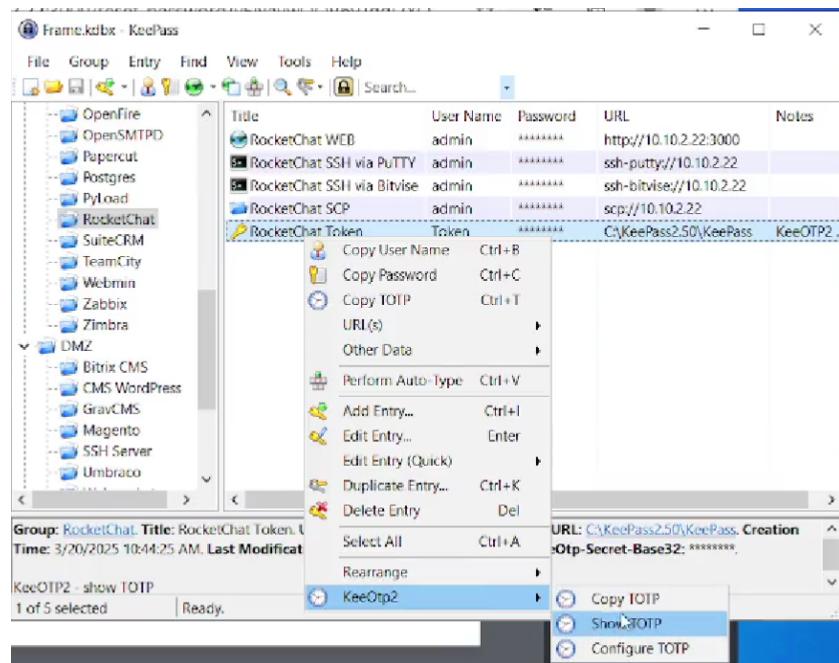


Рис. 31: Генерация одноразового пароля



Рис. 32: Генерация одноразового пароля

Если при введении токена всплывает ошибка, то игнорируя ее, необходимо осуществить вход под новым паролем (рис. 33).

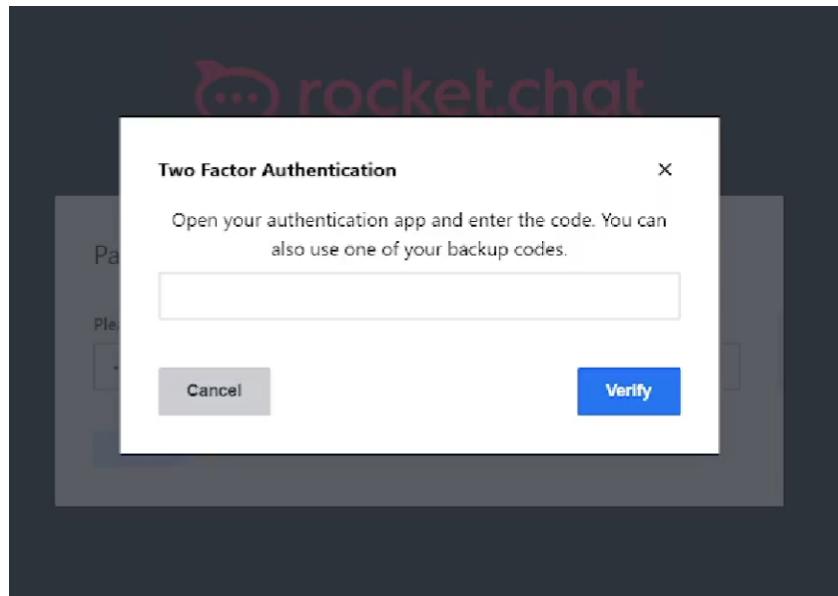


Рис. 33: Двухфакторная аутентификация

**Закрытие без обновления.** Так как вторая NoSQL-инъекция для повышения привилегий использует высокоуровневый оператор БД where, временной, смягчающей мерой, может стать отключение выполнения JavaScript на стороне сервера базы данных. Для этого необходимо отредактировать файл конфигурации БД /etc/mongod.conf, добавив строчку javascriptEnabled: false (рис. 34).

```
admin@rocket-chat-server: ~
GNU nano 4.3          /etc/mongod.conf      Modified
destination: file
logAppend: true
path: /var/log/mongodb/mongod.log

# network interfaces
net:
  port: 27017
  bindIp: 127.0.0.1

# how the process runs
processManagement:
  timeZoneInfo: /usr/share/zoneinfo

#security:
  javascriptEnabled: false
```

Рис. 34: Настройка конфигурации БД

## Обнаружение и нейтрализация полезных нагрузок

Meterpreter-сессия. Цель данной полезной нагрузки - получение нарушителем shell-сессии с уязвимым сервером. Данную полезную нагрузку можно обнаружить при выводе сетевой статистики с помощью утилиты ss и параметрами -tp (позволяет просматривать сведения по TCP-соединениям, список процессов в данный момент). В случае установления соединения, на уязвимой машине появится сокет с машиной нарушителя. Нейтрализовать meterpreter-сессию также можно при помощи утилиты ss с ключом -K, чтобы завершить все сессии с машиной нарушителя необходимо ввести: sudo ss -K dst HACKER\_IP dport = HACKER\_PORT (рис. 35).

```
root@rocket-chat-server:~# ss -tp
State Recv-Q Send-Q Local Address:Port          Peer Address:Port
Process
ESTAB  0        0      10.10.2.22:57212      195.239.174.11:5559
users:(("testsystem",pid=1848,fd=3))
ESTAB  0        0      10.10.2.22:ssh        10.10.2.254:5837
users:(("sshd",pid=9088,fd=4),("sshd",pid=8967,fd=4))
ESTAB  0        64     10.10.2.22:ssh        10.10.2.254:47014
users:(("sshd",pid=7236,fd=4),("sshd",pid=7148,fd=4))
ESTAB  0        0      10.10.2.22:3000      10.10.2.254:5604
users:(("node",pid=681,fd=21))
root@rocket-chat-server:~# ss -K dst 195.239.174.11 dport=5559
Error: an inet prefix is expected rather than "dport=5559".
Cannot parse dst/src address.
root@rocket-chat-server:~# ss -K dst 195.239.174.11 dport = 5559
Netid State Recv-Q Send-Q Local Address:Port          Peer Address:Port Process
tcp   ESTAB  0        0      10.10.2.22:57212      195.239.174.11:5559
root@rocket-chat-server:~#
```

Рис. 35: Пример сокета с узлом нарушителя

Уязвимость и последствия RocketChat устраниены (рис. 36).

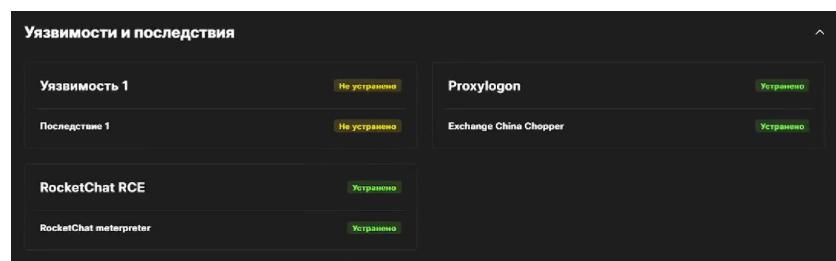


Рис. 36: Уязвимость и последствия устраниены

## Карточки инцидентов

Карточка инцидента WP Discuz RCE (рис. 37).

WP Discuz RCE

Основная информация Чат Закрытый

Дата и время события ①  
27.09.2025 20:34

Описание ①  
Уязвимость CVE-2020-24186 в плагине wpDiscuz для WordPress позволяют неавторизованным пользователям загружать файлы любого типа, включая PHP-файлы, через действие AJAX wmuUploadFiles.

Индикаторы компрометации ①  
AM EXPLOIT WordPress wpDiscuz 7.0.4 RCE and Shell Upload (CVE-2020-24186)

Рекомендации ①  
- отключение плагина через панель администратора CMS WordPress; - обновление плагина до версии 7.0.5 и выше.

Оценка ★ ★ ★ ★ ★  
Автор Аскеров Александр @1132226538@ptfir.ru  
Ответственный Аскеров Александр @1132226538@ptfir.ru  
Источник 195.239.174.11  
Пораженные активы 10.10.1.22

Рис. 37: WP Discuz RCE

Карточка инцидента Proxylogon (рис. 38).

Proxylogon

Основная информация Чат Закрытый

Дата и время события ①  
30.09.2025 15:29

Описание ①  
Proxylogon представляет собой SSRF уязвимость, позволяющую обойти аутентификацию и выдать себя за Администратора.

Индикаторы компрометации ①  
ET TROJAN

Рекомендации ①  
- закрыть доступ к Панели управления Exchange (Exchange Control Panel); - установить обновление из каталога центра обновлений Microsoft.)

Оценка ★ ★ ★ ★ ★  
Автор Аскеров Александр @1132226538@ptfir.ru  
Ответственный Аскеров Александр @1132226538@ptfir.ru  
Источник 195.239.174.11  
Пораженные активы 10.10.1.22

Рис. 38: Proxylogon

Карточка инцидента Rocketchat RCE (рис. 39).

The screenshot shows a dark-themed web interface for a security incident. At the top, it says 'Rocketchat RCE'. Below that, there are tabs for 'Основная информация' (Main Information) and 'Чат' (Chat), with 'Основная информация' being the active tab. A red button labeled 'Закрытый' (Closed) is in the top right corner.

**Основная информация**

**Дата и время события** 30.09.2025 21:21

**Описание**  
CVE-2021-22911 представляет собой две уязвимости NoSQL injection, эксплуатация которых может позволить злоумышленникам повысить свои привилегии, выполнить произвольные системные команды на хост-сервере и украдь конфиденциальные пользовательские данные и сообщения чата. Обе уязвимости исправлены в версии 3.13.2 и перенесены в старые ветки в версиях 3.12.4 и 3.11.4

**Индикаторы компрометации**  
AM EXPLOIT Token BruteForce in RocketChat 3.12.1

**Рекомендации**  
- обновление версии «RocketChat»; - запрет выполнения JavaScript на стороне сервера БД.

**Оценка**  
☆ ☆ ☆ ☆

**Автор**  
Аскрова Александр  
@1152226538@ptiir.ru

**Ответственный**  
Аскрова Александр  
@1152226538@ptiir.ru

**Источник**  
195.239.174.11

**Пораженные активы**  
10.10.2.22

Рис. 39: Rocketchat RCE

## **Вывод**

В ходе выполнения данной лабораторной работы мы исследовали сценарии целенаправленной атаки на корпоративный мессенджер и сопутствующие сервисы, выявили и продемонстрировали эксплуатацию реальных уязвимостей (WpDiscuz, ProxyLogon, RocketChat), а также отработали методы обнаружения, локализации и нейтрализации последствий компрометации для восстановления безопасности информационной инфраструктуры организации.

# **Список литературы**

1. ПОЛНОЕ ОПИСАНИЕ УЯЗВИМОГО УЗЛА «WPDISCUZ». Программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак Ampire».
2. ПОЛНОЕ ОПИСАНИЕ УЯЗВИМОГО УЗЛА «PROXYLOGON» (CVE 2020-26855). Программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак Ampire».
3. ПОЛНОЕ ОПИСАНИЕ УЯЗВИМОГО УЗЛА «ROCKETCHAT». Программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак Ampire».