

Лабораторная работа 1-В

Кибербезопасность предприятия

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

1 октября 2025 г.

Российский университет дружбы народов, Москва, Россия

Наша команда

- НПИбд-01-22
- Российский университет дружбы народов

Цель тренировки

Разобраться с сценарием действий нарушителя “Защита данных сегмента АСУ ТП”. Выявить и устранить уязвимости и их последствия.

Выявленные уязвимости и последствия

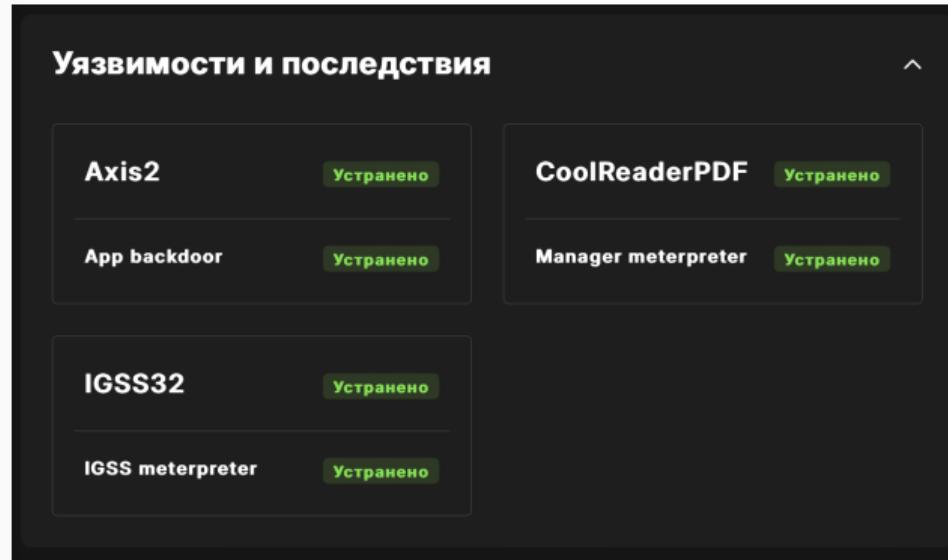


Рис. 1: Уязвимости и последствия

Уязвимая версия axis2

Уязвимая версия axis2 установлена на AppServer под управлением Apache Tomcat. В типовом шаблоне информационной системы используется для развертывания веб-сервисов, работает через порт 8080.

Эксплуатируемая уязвимость – CVE-2010-0219. Компонент Axis2 SAP BusinessObjects содержит учетную запись и пароль администратора по умолчанию.

Из конфигурационного файла axis2.xml можно получить данные учетной записи администратора, авторизоваться и загрузить вредоносный сервис для исполнения команды

Описание инцидента

The screenshot shows the VipNet IDS NS application interface. On the left, there is a list of events with a header 'События' and a dropdown filter 'События за последние 24 часа'. The list includes columns: У..., Дата и время, Код события..., К..., Название правила, and Класс. A single event is selected, highlighted with a blue border, showing the following details:

У...	Дата и время	Код события...	К...	Название правила	Класс
●	08:03:01.827 20...	3006394	1	AM POLICY Apache Axis2 v...	attempted-admin

To the right, a detailed view of the selected event is shown in a modal window titled 'Событие 08:03:01.827 20.09.2025'. The window has tabs at the top: Событие, Источник, Получатель, and Пакет. The 'Событие' tab is active, displaying the following information:

Общая информация	
Дата и время	08:03:01.827 20.09.2025
Интерфейс захвата	eth2
Уровень важности	Высокий
Тип события	Сигнатурное событие
Протокол	TCP
Код события	3006394
Клиентское приложение	Mozilla/5.0 (Macintosh; Intel Mac OS X 13_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36
Доменное имя ресурса	195.239.174.97:8080

Below this, another section titled 'Правило анализа' (Analysis rule) is visible, showing 'Класс' (Class) as 'attempted-admin' and 'Группа' (Group) as 'policy'.

Рис. 2: Событие на VipNet IDS NS

Описание инцидента

Добавление инцидента

Название ⓘ	Дата и время события ⓘ
Уязвимая версия axis2	20.09.2025 08:03
Источник ⓘ	Поражённые активы ⓘ
195.239.174.11 (Kali) x	10.10.1.24 (Apache Tomcat) x
Описание ⓘ	Рекомендации ⓘ
Уязвимая версия axis2 установлена на AppServer под управлением Apache Tomcat. В типовом шаблоне информационной системы используется для развертывания веб-сервисов, работает через порт 80.	- Настройка правила в Iptables, которое отказывает в доступе к конфигурационному файлу при наличии в заголовке строки axis2.xml; - Обновить axis2 до последней версии.
Индикаторы компрометации ⓘ	
AM POLICY Apache Axis2 v1.6 Default Admin Creden	
Прикрепить файл ⓘ	
IDS_packet_time-2025-09-20T05_03_01.827931Z_ruleid-3006394.pcap x	
Выберите файл	
Отмена Добавить	

Рис. 3: Добавление инцидента axis2

Решение

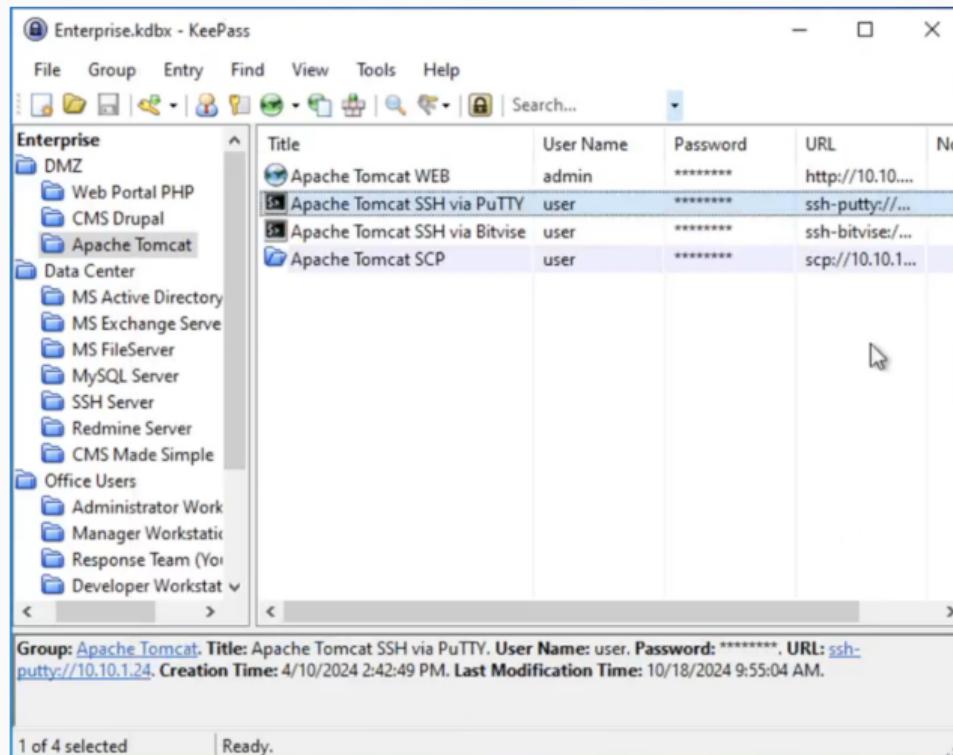
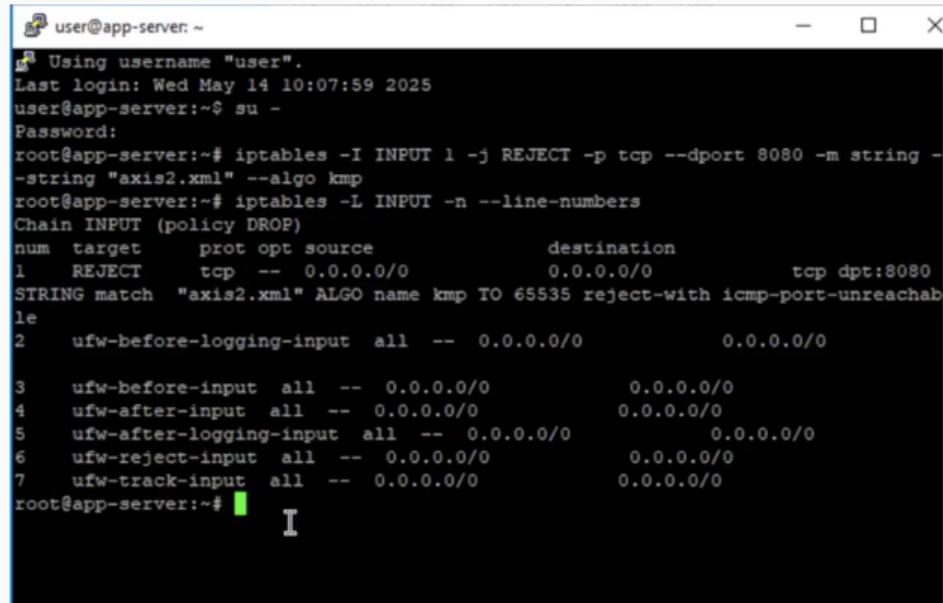


Рис. 4: Подключение по ssh

Решение



The screenshot shows a terminal window titled "user@app-server: ~". The user logs in as "user" and then switches to root using "su -". The root shell shows the command "iptables -I INPUT 1 -j REJECT -p tcp --dport 8080 -m string --string "axis2.xml" --algo kmp" being run. This command adds a new rule to the INPUT chain that rejects TCP traffic on port 8080 if it contains the string "axis2.xml" using the KMP algorithm. The output also shows the current state of the INPUT chain, which includes rules for ufw and other standard Linux services.

```
user@app-server: ~
Using username "user".
Last login: Wed May 14 10:07:59 2025
user@app-server:~$ su -
root@app-server:~# iptables -I INPUT 1 -j REJECT -p tcp --dport 8080 -m string --string "axis2.xml" --algo kmp
root@app-server:~# iptables -L INPUT -n --line-numbers
Chain INPUT (policy DROP)
num  target     prot opt source          destination
1    REJECT     tcp  --  0.0.0.0/0      0.0.0.0/0          tcp dpt:8080
STRING match  "axis2.xml" ALGO name kmp TO 65535 reject-with icmp-port-unreachable
2    ufw-before-logging-input  all  --  0.0.0.0/0      0.0.0.0/0
3    ufw-before-input  all  --  0.0.0.0/0      0.0.0.0/0
4    ufw-after-input  all  --  0.0.0.0/0      0.0.0.0/0
5    ufw-after-logging-input  all  --  0.0.0.0/0      0.0.0.0/0
6    ufw-reject-input  all  --  0.0.0.0/0      0.0.0.0/0
7    ufw-track-input  all  --  0.0.0.0/0      0.0.0.0/0
root@app-server:~#
```

Рис. 5: Добавление правила в утилите

Решение

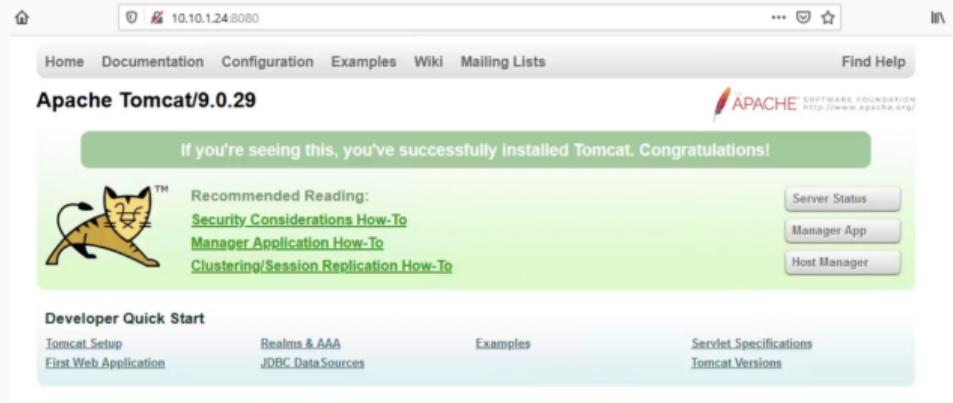


Рис. 6: Стартовая страница сервера Apache Tomcat

Решение

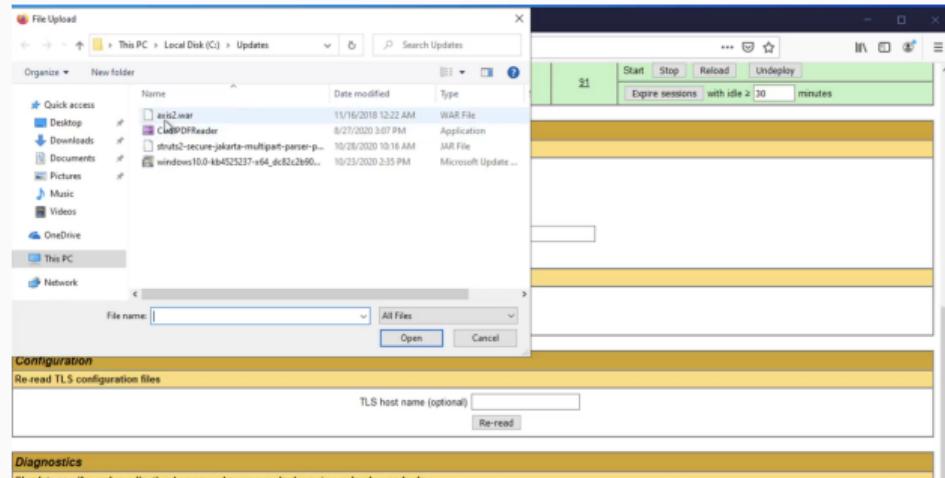


Рис. 7: Добавление axis2.war

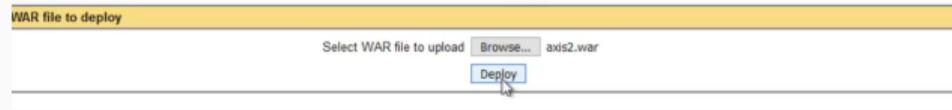


Рис. 8: Нажатие на кнопку

Последствия App Backdoor

```

listening-socket=1 FWD:88 -t8
State Recv-Q Send-Q Local Address:Port          Peer Address:Port
CLOSING 1 190 17.0.0.1:154056 17.0.0.1:ihhttp-alt
ESTAB 0 0 10.10.1.24:57430 10.16.2.17:52094 users=(({"egg_agentd",pid=1064,fd=55})
CLOSING 1 190 17.0.0.1:154093 17.0.0.1:ihhttp-alt
ESTAB 1 190 17.0.0.1:154093 17.0.0.1:ihhttp-alt
ESTAB 0 64 10.10.1.24:57430 10.10.1.251:70555 users=(({"ashd",pid=31087,fd=3}, {"ashd",pid=31003,fd=3}))
FIN_WAIT_1 0 190 17.0.0.1:154940 17.0.0.1:ihhttp-alt
ESTAB 0 0 10.10.1.24:44049 198.239.174.11:7777 users=(({"evil.conf",pid=6504,fd=3}))
CLOSING 1 190 17.0.0.1:154940 17.0.0.1:ihhttp-alt
CLOSING 1 190 17.0.0.1:154934 17.0.0.1:ihhttp-alt
CLOSING 1 190 17.0.0.1:154974 17.0.0.1:ihhttp-alt
FIN_WAIT_1 0 190 17.0.0.1:154926 17.0.0.1:ihhttp-alt
ESTAB 0 0 10.10.1.24:38320 10.16.1.25:10544 users=(({"fileBeat",pid=447,fd=8}))
CLOSING 1 190 17.0.0.1:154940 17.0.0.1:ihhttp-alt
CLOSING 1 190 17.0.0.1:154970 17.0.0.1:ihhttp-alt
CLOSING 1 190 17.0.0.1:154980 17.0.0.1:ihhttp-alt
ESTAB 1 190 17.0.0.1:154766 17.0.0.1:ihhttp-alt
ESTAB 0 0 10.10.1.24:44106 198.239.174.11:11653 users=(({"DtGCD",pid=6535,fd=3}))
CLOSING 1 190 17.0.0.1:154940 17.0.0.1:ihhttp-alt
ESTAB 0 190 17.0.0.1:154938 17.0.0.1:ihhttp-alt
CLOSE_WAIT 1 0 [:ffff:10.10.1.28]:ihhttp-alt [ffff:198.239.174.11:17091] users=(({"python",pid=540,fd=3}), {"java",pid=601,fd=315})
FIN_WAIT_2 0 0 [:ffff:127.0.0.1]:ihhttp-alt [ffff:198.239.174.11:17091] users=(({"java",pid=601,fd=315}))
FIN_WAIT_1 0 20376 [:ffff:10.10.1.28]:ihhttp-alt [ffff:198.239.174.11:17091] users=(({"java",pid=601,fd=315}))
CLOSING 0 0 [:ffff:127.0.0.1]:ihhttp-alt [ffff:198.239.174.11:17091] users=(({"java",pid=601,fd=315}))
FIN_WAIT_2 0 0 [:ffff:127.0.0.1]:ihhttp-alt [ffff:198.239.174.11:17091] users=(({"java",pid=601,fd=315}))
ESTAB 0 0 [:ffff:127.0.0.1]:ihhttp-alt [ffff:198.239.174.11:16926] users=(({"java",pid=601,fd=129}))

```

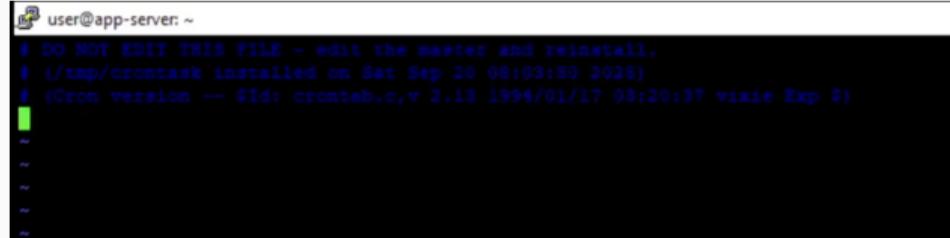
Рис. 9: Установленная сессия с нарушителем

Последствия App Backdoor

```
y.  
Sep 20 12:17:33 localhost systemd[1]: vipnet_epp_bash_monitor.service: Succeeded.  
Sep 20 12:17:33 localhost systemd[1]: Started ViPNet Endpoint Protection Bash Monitor.  
Sep 20 12:17:46 localhost systemd[1]: Starting ViPNet Endpoint Protection Bash Monitor...  
Sep 20 12:17:46 localhost systemd[1]: Configuration file /etc/systemd/system/sc6_struts2.service is ma  
y.  
Sep 20 12:17:47 localhost systemd[1]: vipnet_epp_bash_monitor.service: Succeeded.  
Sep 20 12:17:47 localhost systemd[1]: Started ViPNet Endpoint Protection Bash Monitor.  
Sep 20 12:17:52 localhost systemd[1]: Starting ViPNet Endpoint Protection Bash Monitor...  
Sep 20 12:17:52 localhost systemd[1]: Configuration file /etc/systemd/system/sc6_struts2.service is ma  
y.  
Sep 20 12:17:53 localhost systemd[1]: vipnet_epp_bash_monitor.service: Succeeded.  
Sep 20 12:17:53 localhost systemd[1]: Started ViPNet Endpoint Protection Bash Monitor.  
Sep 20 12:18:01 localhost systemd[1]: Starting ViPNet Endpoint Protection Bash Monitor...  
Sep 20 12:18:01 localhost CRON[9725]: (tomcat) CMD (/opt/tomcat/webapps/evil.conf)  
Sep 20 12:18:01 localhost systemd[1]: Configuration file /etc/systemd/system/sc6_struts2.service is ma  
y.  
user@app-server:~$ █
```

Рис. 10: Автозапуск backdoor

Последствия App Backdoor



A screenshot of a terminal window titled "user@app-server: ~". The window contains the following text:

```
* DO NOT EDIT THIS FILE - edit the master and reinstall.  
* (/tmp/crontask installed on Sat Sep 20 08:03:50 2025)  
* (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)  
[redacted]
```

The terminal window has a black background with white text. The title bar is white with black text. The bottom of the window shows a series of five horizontal bars, with the first one being red.

Рис. 11: Отключение автозапуска

Последствия App Backdoor

```
root@app-server:~# cd /opt/tomcat/webapps/
root@app-server:/opt/tomcat/webapps# rm evil.conf
root@app-server:/opt/tomcat/webapps#
root@app-server:/opt/tomcat/webapps# ss -tp
State      Recv-Q    Send-Q          Local Address:Port          Peer Address:Port
CLOSING     1           0           127.0.0.1:55094          127.0.0.1:https-alt
ESTAB       0           0           10.10.1.24:57630          10.10.2.17:25004      users:(("epp_agentd",pid=1066,fd=1)
CLOSING     1           190          127.0.0.1:55128          127.0.0.1:https-alt
FIR-WAIT-1   0           190          127.0.0.1:55248          127.0.0.1:https-alt
CLOSING     1           190          127.0.0.1:55216          127.0.0.1:https-alt
ESTAB       0           64           10.10.1.24:40498         10.10.1.25:47055      users:(("ashd",pid=31007,fd=3),
ESTAB       0           0           10.10.1.24:40498         10.239.174.11:7777    users:(("evil.conf",pid=5984,fd=4)
CLOSING     1           190          127.0.0.1:55143          127.0.0.1:https-alt
CLOSING     1           190          127.0.0.1:55172          127.0.0.1:https-alt
CLOSING     1           190          127.0.0.1:55154          127.0.0.1:https-alt
FIR-WAIT-1   0           190          127.0.0.1:55238          127.0.0.1:https-alt
ESTAB       0           0           10.10.1.24:38820         10.10.1.25:5044      users:(("filebeat",fd=647,fd=5)
CLOSING     1           190          127.0.0.1:55186          127.0.0.1:https-alt
CLOSING     1           190          127.0.0.1:55202          127.0.0.1:https-alt
CLOSING     1           190          127.0.0.1:55224          127.0.0.1:https-alt
CLOSING     1           190          127.0.0.1:55102          127.0.0.1:https-alt
CLOSING     1           190          127.0.0.1:55112          127.0.0.1:https-alt
ESTAB       0           0           10.10.1.24:44106         195.239.174.11:4433   users:(("DtcOto",pid=5439,fd=3))
FIR-WAIT-2   0           0           [:ffff:127.0.0.1]:https-alt [:ffff:127.0.0.1]:55142
FIR-WAIT-2   0           0           [:ffff:127.0.0.1]:https-alt [:ffff:127.0.0.1]:55126
FIR-WAIT-2   0           0           [:ffff:127.0.0.1]:https-alt [:ffff:127.0.0.1]:55154
ESTAB       0           0           [:ffff:127.0.0.1]:https-alt [:ffff:127.0.0.1]:55156      users:(("java",pid=601,fd=110))
FIR-WAIT-2   0           0           [:ffff:127.0.0.1]:https-alt [:ffff:127.0.0.1]:55224
ESTAB       0           0           [:ffff:10.10.1.24]:https-alt [:ffff:10.10.1.24]:55101      users:(("java",pid=601,fd=315))
ESTAB       0           0           [:ffff:127.0.0.1]:https-alt [:ffff:127.0.0.1]:55238      users:(("java",pid=601,fd=1)
ESTAB       0           0           [:ffff:10.10.1.24]:40424        [:ffff:195.239.174.11]:4427   users:(("java",pid=601,fd=1)
FIR-WAIT-2   0           0           [:ffff:127.0.0.1]:https-alt [:ffff:127.0.0.1]:55196
FIR-WAIT-2   0           0           [:ffff:127.0.0.1]:https-alt [:ffff:127.0.0.1]:55202
FIR-WAIT-2   0           0           [:ffff:127.0.0.1]:https-alt [:ffff:127.0.0.1]:55172
FIR-WAIT-2   0           0           [:ffff:127.0.0.1]:https-alt [:ffff:127.0.0.1]:55234
```

Рис. 12: Удаление исполняемого файла и заверение сессий с машиной нарушителя

Уязвимая версия программы CoolReaderPDF

На хосте Manager Workstation 1 установлена уязвимая версия программы CoolReaderPDF. Хост используется для приема писем по публичной и корпоративной электронной почте. Эксплуатируемая уязвимость – CVE-2012-4914.

Переполнение стека в программе CoolPDFReader позволяет удаленно выполнять код при чтении специально сгенерированного документа. В данном случае сгенерированный документ соединен с некоторым стандартным отчетом. При просмотре последней страницы происходит эксплуатация уязвимости. Уязвимости подвержена программа чтения CoolReaderPDF версии 3.0.2.256, которая позволяет удаленным нарушителям выполнять произвольный код через документ PDF с созданным потоком. При просмотре начальной части документа программа работает стандартно. При попытке просмотра седьмой страницы программа не реагирует на команды пользователя («зависает»), нарушитель получает сессию.

Описание инцидента

The screenshot shows the VipNet IDS NS interface. On the left, there is a list of events titled 'События' (Events) with a dropdown filter set to 'События за последние 24 часа' (Events over the last 24 hours). The list contains four entries, all of which are highlighted in blue. Each entry includes columns for 'У...', 'Дата и время' (Date and time), 'Код события' (Event ID), 'К.' (Severity), 'Название правила' (Rule name), and 'Класс' (Class). The first event is selected, and its details are shown in a larger window on the right.

Событие 08:05:37.715 20.09.2025

Событие	Источник	Получатель	Пакет
уровень важности	высокий		
Тип события	Сигнатурное событие		
Протокол	TCP		
Код события	2025644		

Правило анализа

Класс	trojan-activity
Группа	trojan
Название	ET TROJAN Possible Metasploit Payload Common Construct Bind_API (from server)

Описание:
Правило обнаруживает сетевую активность вредоносного ПО

Текст:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg: "ET TROJAN Possible M etasploit Payload Common Construct Bind_API (from server)";flow: from_server established;content: "60 89 e5 31";content: "64 8b";distance: 1;within: 2;content: "1c 8b 52 14 8b 72 28 0f b7 4a 26 31 ff";dist ance: 1;within: 12;content: "4c 0a 63 7e 09 0a 00 a1 ad 0d 03 a7 a7";within: 1;dist
```

Рис. 13: Событие на VipNet IDS NS

Описание инцидента

Добавление инцидента

Название ⓘ
Уязвимая версия программы CoolReaderPDF

Дата и время события ⓘ
20.09.2025 08:05

Источник ⓘ
195.239.174.11 (Kali) ×

Поражённые активы ⓘ
10.10.4.11 (Manager Workstation 1) ×

Описание ⓘ
Переполнение стека в программе CoolPDFReader позволяет удаленно выполнять код при чтении специально сгенерированного документа.

Рекомендации ⓘ
В Windows Firewall добавить правило, блокирующее входящий/исходящий трафик от программы CoolPDFReader, обновить программу CoolReaderPDF до последней версии.
Аналогично выставляется для входящего

Индикаторы компрометации ⓘ
На машине менеджера открыто приложение и оно

Прикрепить файл ⓘ

Перетяните файл в эту область или
Выберите файл

Отмена Добавить

Рис. 14: Добавление инцидента CoolReaderPDF

Решение

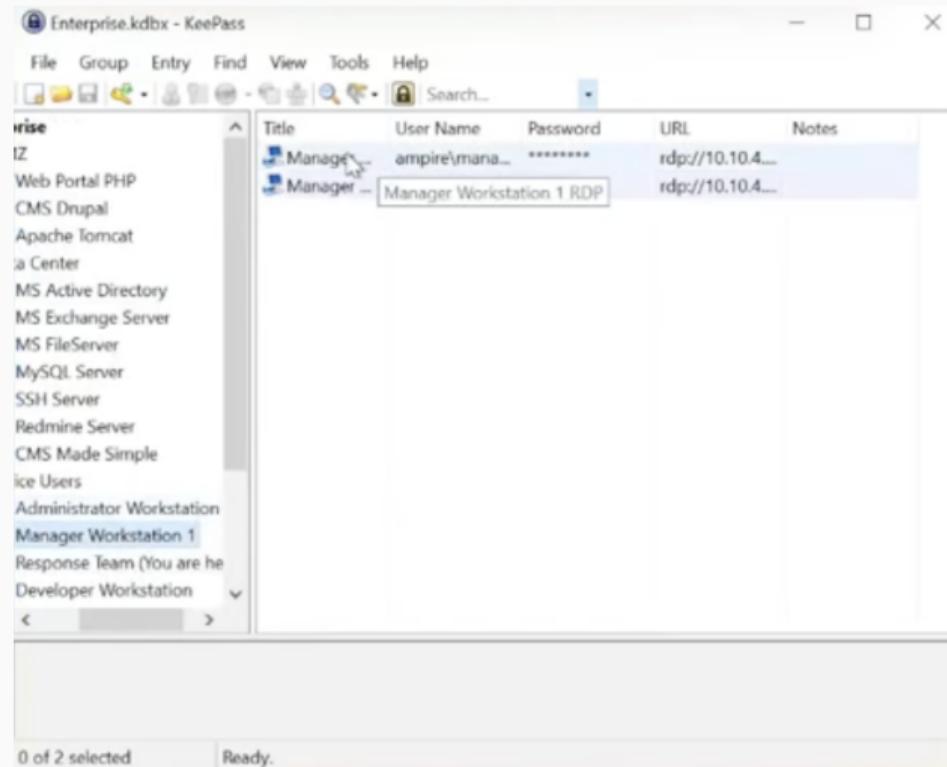


Рис. 15: Подключение к Manager Workstation 1

Решение

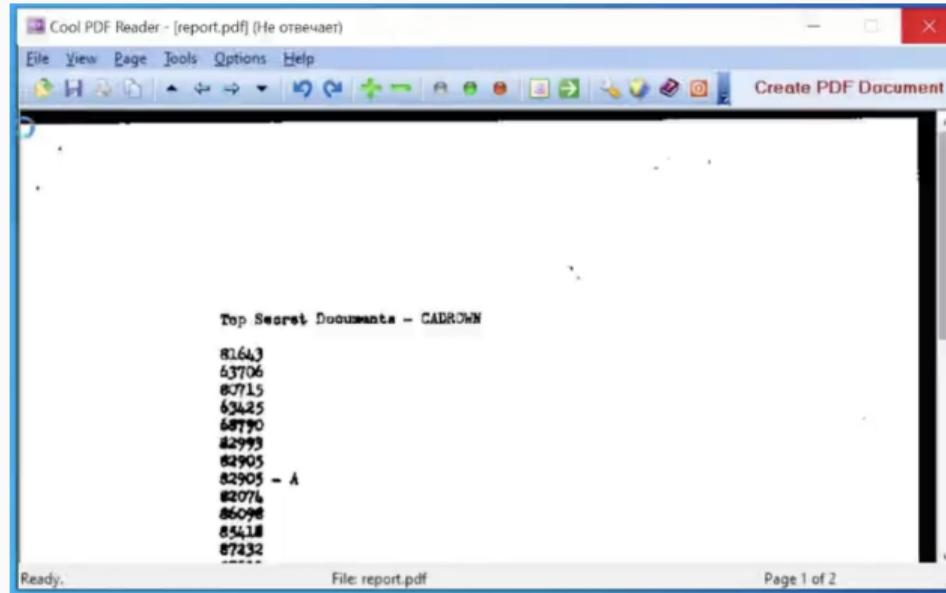


Рис. 16: Ошибка

Решение

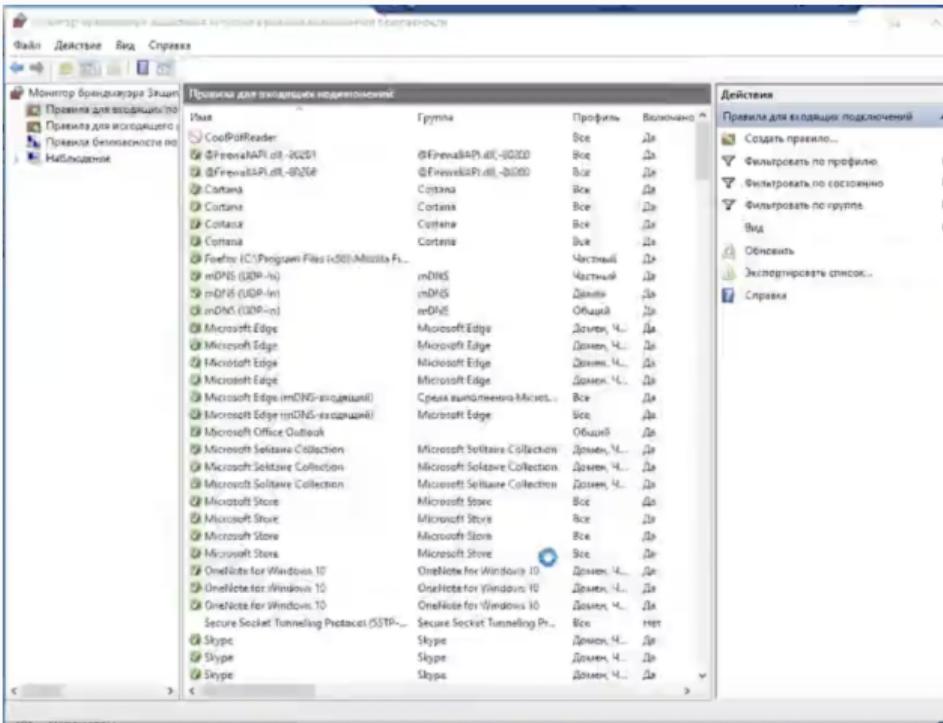


Рис. 17: Добавленное правило

Решение

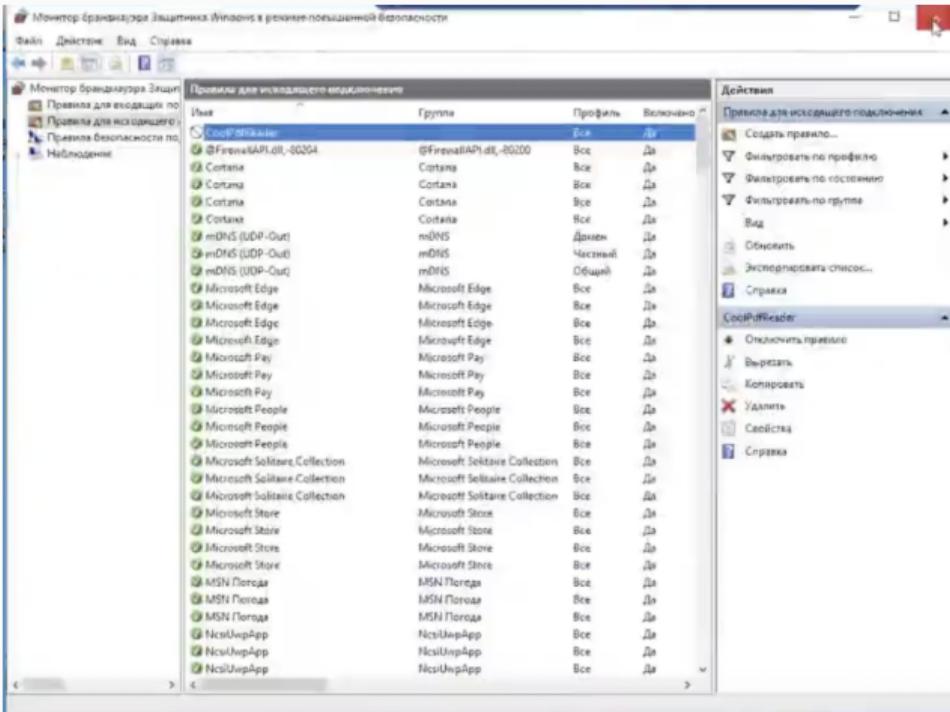


Рис. 18: Добавленное правило

Последствия Manager meterpreter

C:\Users\administrator>netstat -ano				
Активные подключения				
Имя	Локальный адрес	Внешний адрес	Состояние	PID
TermService [svchost.exe]	TCP 10.10.4.11:3389	10.10.4.12:51946	ESTABLISHED	528
[OUTLOOK.EXE]	TCP 10.10.4.11:52635	10.10.2.11:443	ESTABLISHED	5292
[CoolPDFReader.exe]	TCP 10.10.4.11:52701	195.239.174.11:4445	ESTABLISHED	4776
	TCP 10.10.4.11:52738	10.10.2.11:443	TIME_WAIT	0
	TCP 10.10.4.11:53759	195.239.174.12:443	TIME_WAIT	0
	TCP 10.10.4.11:53760	195.239.174.12:443	TIME_WAIT	0
	TCP 10.10.4.11:53761	10.10.1.21:80	TIME_WAIT	0
	TCP 10.10.4.11:53762	195.239.174.12:443	TIME_WAIT	0

Рис. 19: Список установленных соединений

Последствия Manager meterpreter

```
C:\Users\administrator>taskkill /f /pid 4776
Успешно: Процесс с идентификатором 4776, успешно завершен.

C:\Users\administrator>
```

Рис. 20: Остановка процесса

Эксплуатируемая уязвимость – CVE-2011-1567.

Переполнение стека в программе с графическим интерфейсом IGSSdataServer.exe при использовании операции ListAll ведет к удаленному выполнению кода и прямому подключению нарушителя к серверу.

Описание инцидента

The screenshot shows two windows from the VipNet IDS NS interface. The left window is titled 'События' (Events) and displays a list of recent events. The right window is a detailed view of a specific event, titled 'Событие 08:05:27.368 20.09.2025'. This detailed view includes sections for 'Общая информация' (General information), 'Правило анализа' (Analysis rule), and a description of the exploit.

У...	Дата и время	Код события	К...	Название правила	Класс
●	08:05:27.368 20...	3006078	1	AM Exploit 7T Interactive Gr...	web-application-at...
●	08:05:27.368 20...	3006078	1	AM Exploit 7T Interactive Gr...	web-application-at...

Событие 08:05:27.368 20.09.2025

Событие	Источник	Получатель	Пакет
Общая информация			
Дата и время	08:05:27.368 20.09.2025		
Интерфейс захвата	eth2		
Уровень важности	Высокий		
Тип события	Сигнатурное событие		
Протокол	TCP		
Код события	3006078		
Правило анализа			
Класс	web-application-attack		
Группа	exploit		
Название	AM Exploit 7T Interactive Graphical SCADA Buffer Overflow 0d		
Описание:	Правило обнаруживает в сетевом трафике программный код, предназначенный для эксплуатации уязвимости		

Рис. 21: Событие на VipNet IDS NS

Описание инцидента

The screenshot shows a 'Добавление инцидента' (Add incident) form. It includes fields for 'Название' (Name) and 'Дата и время события' (Event date and time). A note at the bottom states 'Уязвимая версия IGSS' (Vulnerable version of IGSS).

Добавление инцидента

Название ⓘ

Дата и время события ⓘ

Уязвимая версия IGSS

20.09.2025 08:05

Решение

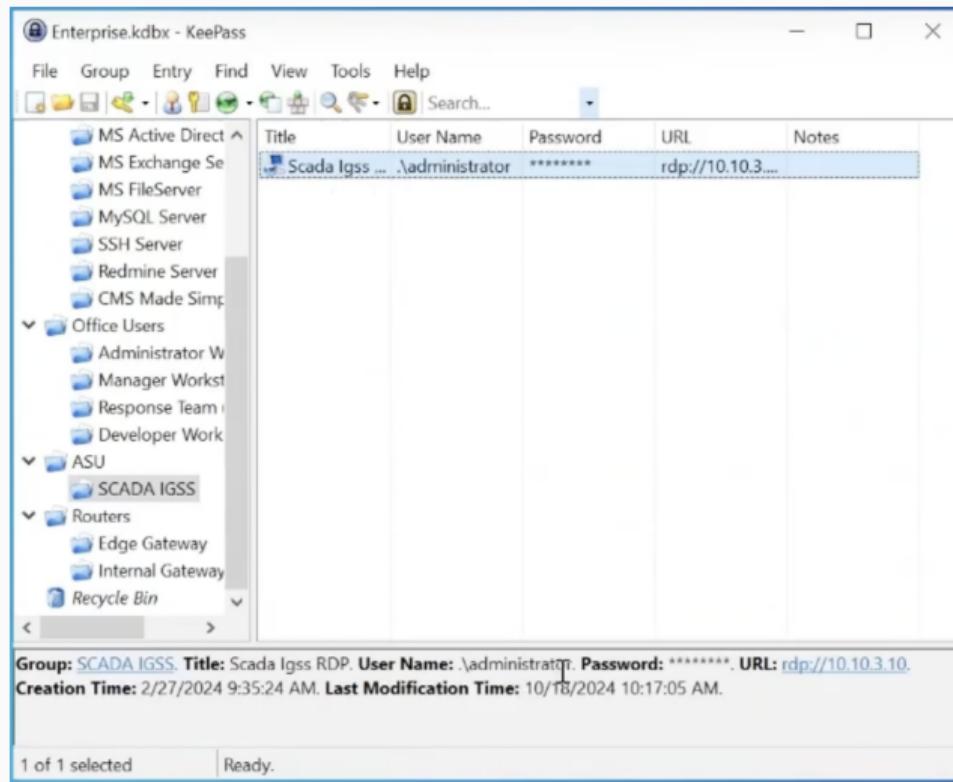
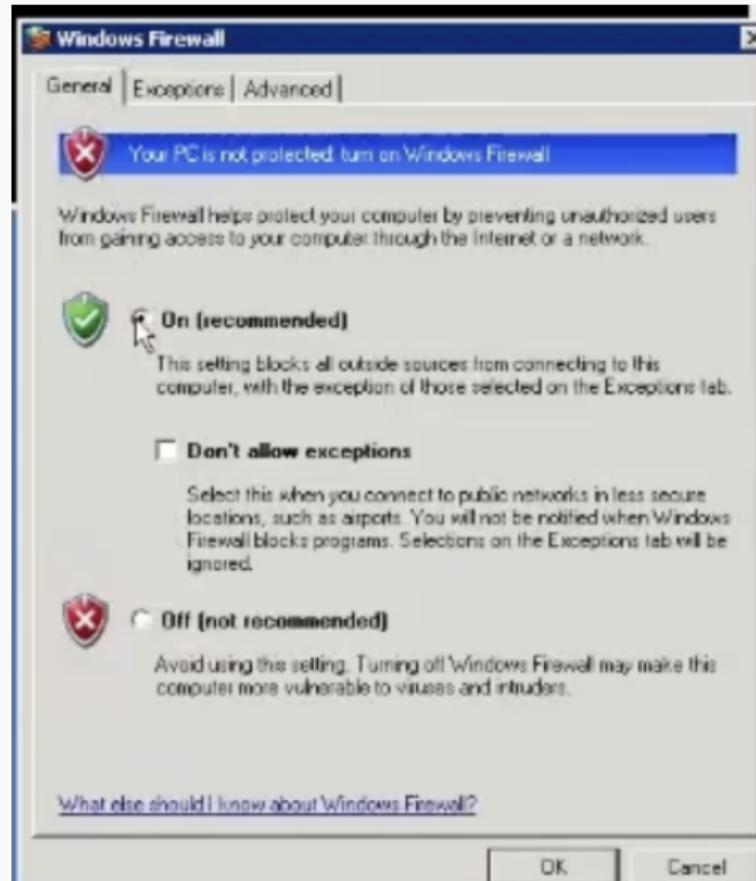
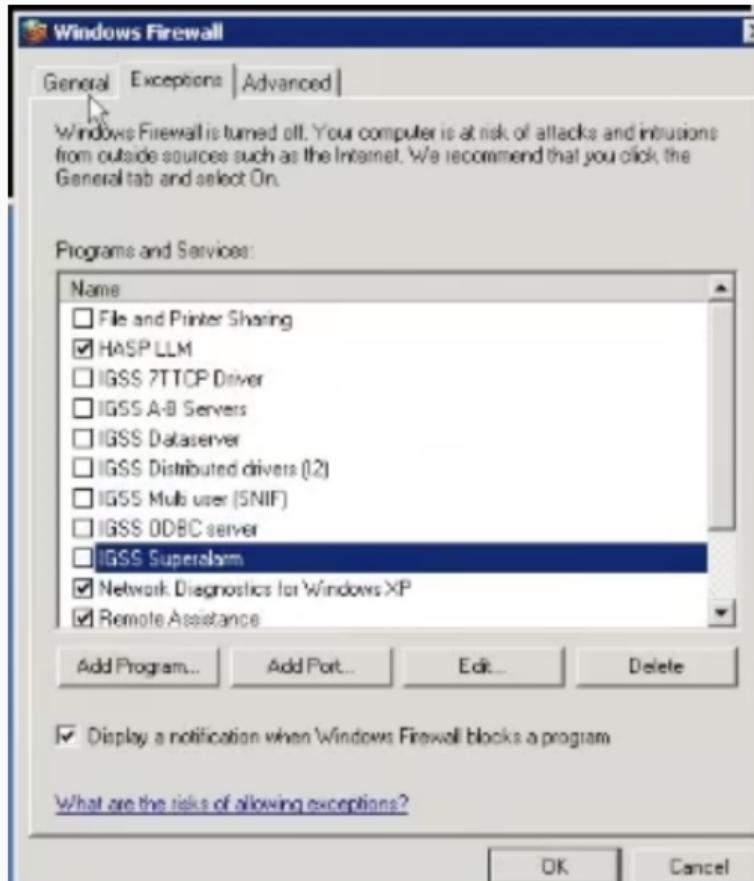


Рис. 23: Подключение



Решение



Последствия IGSS meterpreter

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>netstat -ano

Active Connections

 Proto  Local Address          Foreign Address        State      PID
 TCP    10.10.3.10:4141        195.239.174.11:20002  ESTABLISHED 1212
 [IGSSdataServer.exe]

 TCP    10.10.3.10:3389        10.10.4.12:51868      ESTABLISHED 868
 -- unknown component(s) --
 [svchost.exe]

 TCP    127.0.0.1:2745         127.0.0.1:12481       TIME_WAIT   0
 TCP    127.0.0.1:2746         127.0.0.1:12481       TIME_WAIT   0
 TCP    127.0.0.1:2254         127.0.0.1:12481       TIME_WAIT   0
 TCP    127.0.0.1:2755         127.0.0.1:12481       TIME_WAIT   0

C:\Documents and Settings\Administrator>
```

Рис. 26: Соединение с машиной нарушителя

Последствия IGSS meterpreter

```
C:\Documents and Settings\Administrator>taskkill /f /pid 1212
SUCCESS: The process with PID 1212 has been terminated.

C:\Documents and Settings\Administrator>
```

Вывод

Получили навыки настройки VPN-туннеля через незащищённое Интернет соединение.