Верификация SSRF эксплуатации

Бейбутов Эльдар

Эксперт Positive Technologies

Поиск уязвимостей

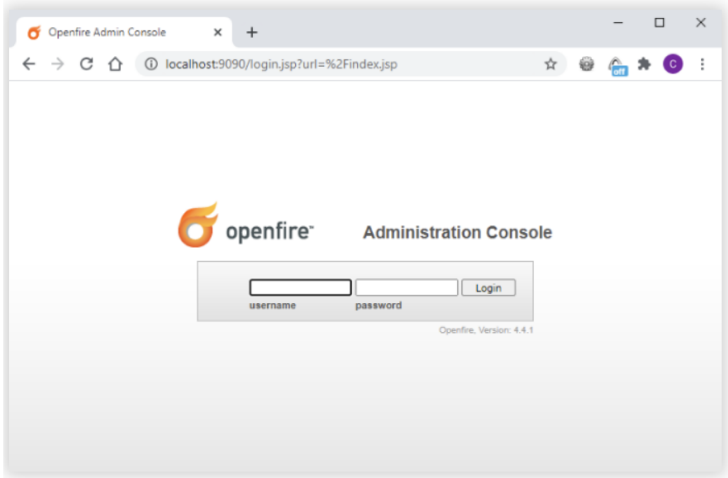
PT SWARM Home About

Vulnerabilities in the Openfire Admin Console

Written by Alexandr Shvetsov on August 4, 2020

Openfire is a Jabber server supported by Ignite Realtime. It's a cross-platform Java application, which positions itself as a platform for medium-sized enterprises to control internal communications and make instant messaging easier.

I regularly see Openfire on penetration testing engagements, and most of the time all interfaces of this system are exposed to an external attacker, including the administrative interface on 9090/http and 9091/https ports:



Openfire Administration Console

Since the Openfire system is available on GitHub, I decided to examine the code of this web interface. This is a short writeup about two vulnerabilities I was able to find.

Alexandr Shvetsov
Penetration Testing Expert
shvetsovalex007

An HHTP request to test the vulnerability:

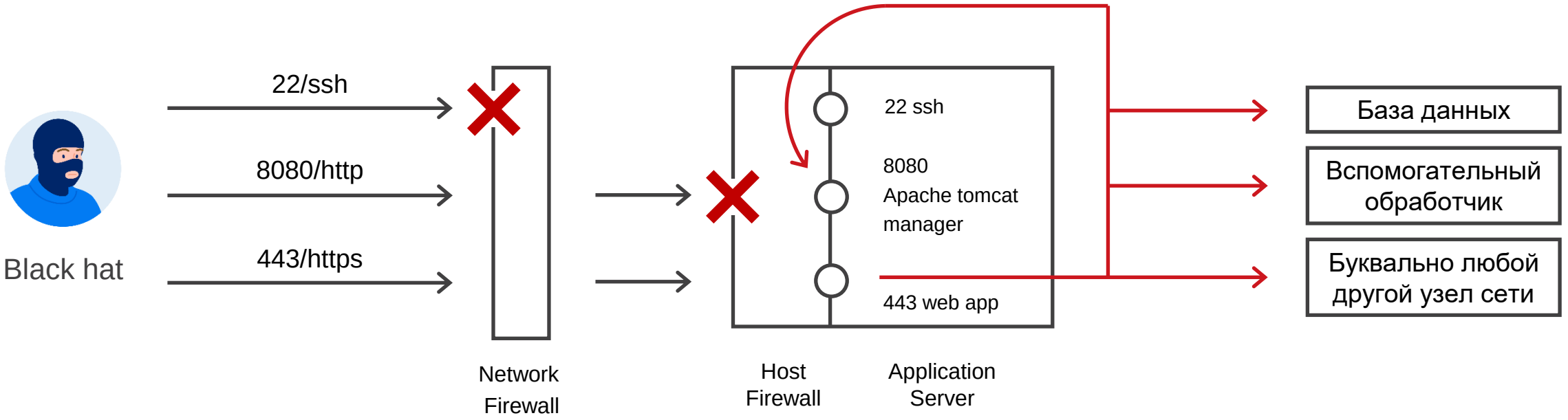
```
GET /getFavicon?host=192.168.176.1:8080/secrets.txt? HTTP/1.1
Host: assesmenthost.com:9090
```

An example of a vulnerable server’s behavior:

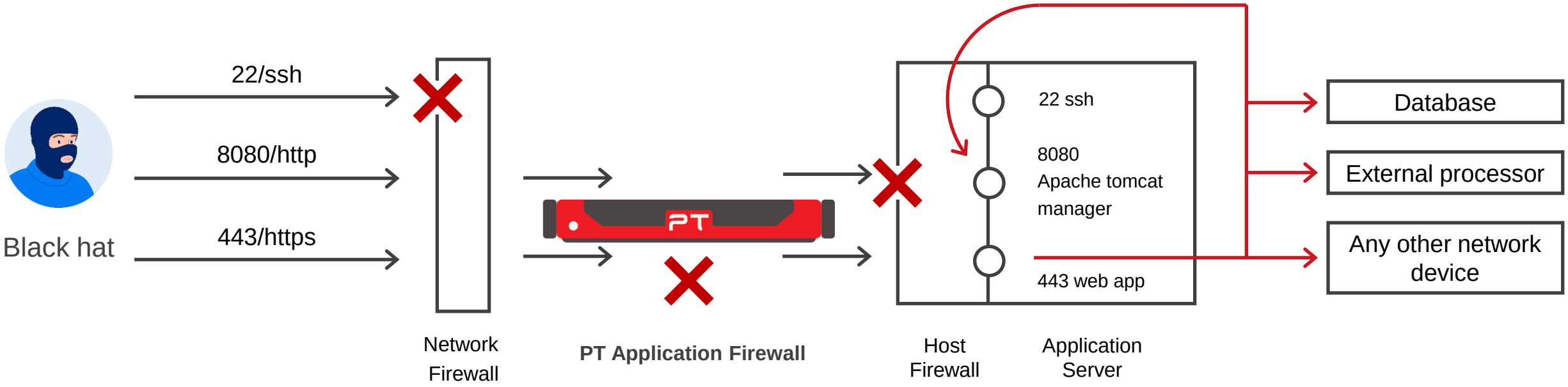
An example of CVE-2019-18392 exploitation in Burp Suite

URL Components(RFC 3986)

SSRF — в чем опасность?



WAF approach



Разные сценарии WAF

Зрелость потребности:

- Компания ищет серебряную пулю, универсальное решение, которое поможет снизить уровень риска без значительных вложений в экспертизу и команду. WAF может выглядеть в их глазах как антивирус, использовать конфигурацию по умолчанию, и надеяться, что это увеличит стоимость атаки и, соответственно, взлом системы может выглядеть менее привлекательно в глазах злоумышленника.

Назовем это Cloud WAF, потому что облачные сервисы этого типа обычно нацелены на достижение этой цели, тем не менее, on-prem решение также способно реализовать такой сценарий.

- Компания знает большинство слабых мест в своих приложениях путем регулярного анализа безопасности, поиска определенных технологий, которые помогут создать виртуальный патч и обеспечить безопасность приложения, пока разработчики исправляют ошибку.

Назовем это Virtual patching WAF.

- Компания использует подход SOC security и нуждается в богатых и мощных инструментах, которые будут извлекать данные для корреляций инцидентов.

Назовем это SOC WAF.

Что если Cloud WAF?

1. Индентификация Jabber сервера openfire версии 4.4.1
2. Попытка эксплуатации CVE-2019-18393 — **неуспешная**
3. Исследование других аспектов безопасности:
   - Brute force / Credential stuffing атака
   - Недостатки сессионного механизма
   - Небезопасное восстановление пароля
   - Вирусное заражение администратора

   } **Повышение стоимости атаки**
4. Вход в панель администратора
5. Установка плагина с произвольным исполняемым кодом, **Remote Code Execution**

Что если Cloud WAF?

Компания только собирается провести анализ защищенности приложений или недавно провела первый

WAF устанавливается с настройками «по-умолчанию» в режиме блокировки

WAF рассматривается как средство повышения стоимости атаки

Демо

Плюсы	Минусы
Все приложения получают комлексную защиту от типовых атак	Блокировка подозрительных запросов ведёт к деградации приложения, что приводит к необходимости писать исключения Не всегда стоимость повышается равномерно по плоскости атаки, что может привести к пробою

Virtual Patch security

- Текущая внутренняя разработка
- Купленное, поддерживаемое

Сообщить о уязвимости

Дождаться патч

Обновить приложение

От 1 до 36 месяцев

- Купленное, неподдерживаемое
- Доставшиеся по наследству
- С открытым исходным кодом

Невозможно определить ответственного

Уязвимость перманентна

Что если VP WAF?

1. Индентификация Jabber сервера openfire версии 4.4.1
2. Попытка эксплуатации CVE-2019-18393 — **неуспешная**
3. Исследование других аспектов безопасности:
   - Brute force / Credential stuffing атака
   - Недостатки сессионного механизма
   - Небезопасное восстановление пароля
   - Вирусное заражение администратора

   } **Повышение стоимости атаки!**
4. Вход в панель администратора
5. Установка плагина с произвольным исполняемым кодом, **неуспешно**

Что если VP WAF?

Компания регулярно проводит анализ защищенности приложений

WAF рассматривается как средство сокращения времени закрытия уязвимостей

Демо

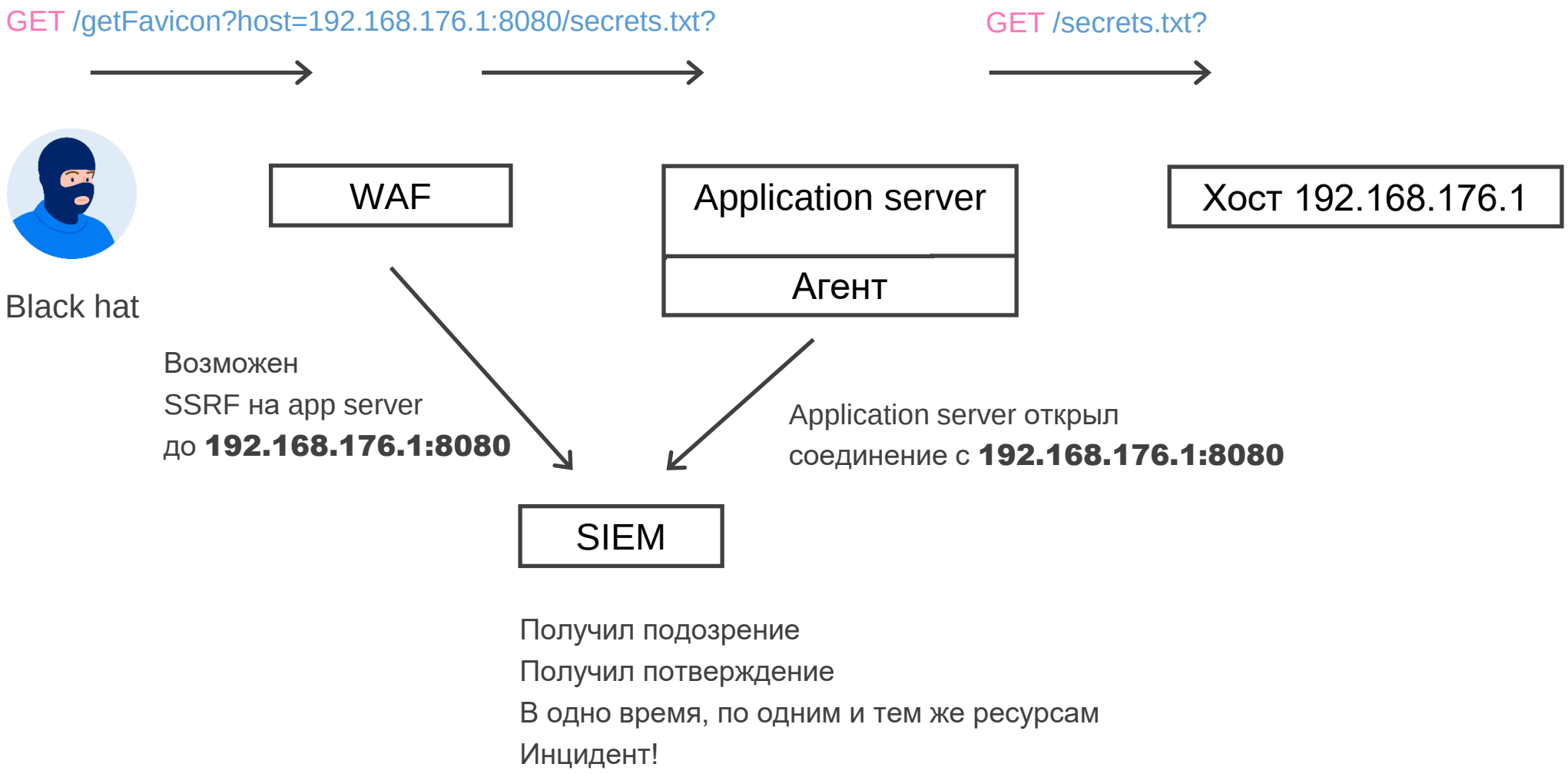
Плюсы	Минусы
Блокируются только атаки	На поиск и устранение уязвимостей понадобиться отдельный человек/команда
Приложения одсмотрены с точки зрения злоумышленника, разрушены критичные для цепочки атаки звенья	Всегда будет естественный лаг, между рождением и устранением уязвимости, в который могут попасть злоумышленники и реализовать атаку
Процессы ведут к изучению своих приложений и их уяявзимостей	

Что если SOC WAF?

1. Индентификация Jabber сервера openfire версии 4.4.1
2. **Попытка эксплуатации CVE-2019-18393** — **неуспешная**
3. Исследование других аспектов безопасности:
   - Brute force / Credential stuffing атака
   - Недостатки сессионного механизма
   - Небезопасное восстановление пароля
   - Вирусное заражение администратора

   } **Повышение стоимости атаки!**
4. Вход в панель администратора
5. **Установка плагина с произвольным исполняемым кодом**, **неуспешно**

SOC security



SOC security

POST /install_plugin.php

Black hat

WAF

Application server

Агент

POST Запрос

Изменения в директории с исполняемым кодом

SIEM

Получил подозрение
Получил потверждение
В одно время, по одним и тем же ресурсам
Инцидент!

SOC security

Описание кейса

Компания серьезна обеспокоена собственной безопасностью, внедрены все необходимые средства защиты и объединены в так называемый SOC (security operation center)

WAF рассматривается как элемент системы по контролю за инфраструктурой

Основная задача не блокировка атак, а контроль злоумышленника в инфраструктуре, предотвратить наступление недопустимого ущерба.

Плюсы	Минусы
Ничего не блокируется Контроль уязвимостей становится менее критичен, так как мониторинг настроен на инцидентную модель Обнаружение уязвимостей в момент их эксплуатации	В систему входит большое количество компонент, которые должны управляться командой экспертов, SIEM, NTA, EDP, WAF, etc