Мировые тренды ИБ

на службе ФинЦЕРТ

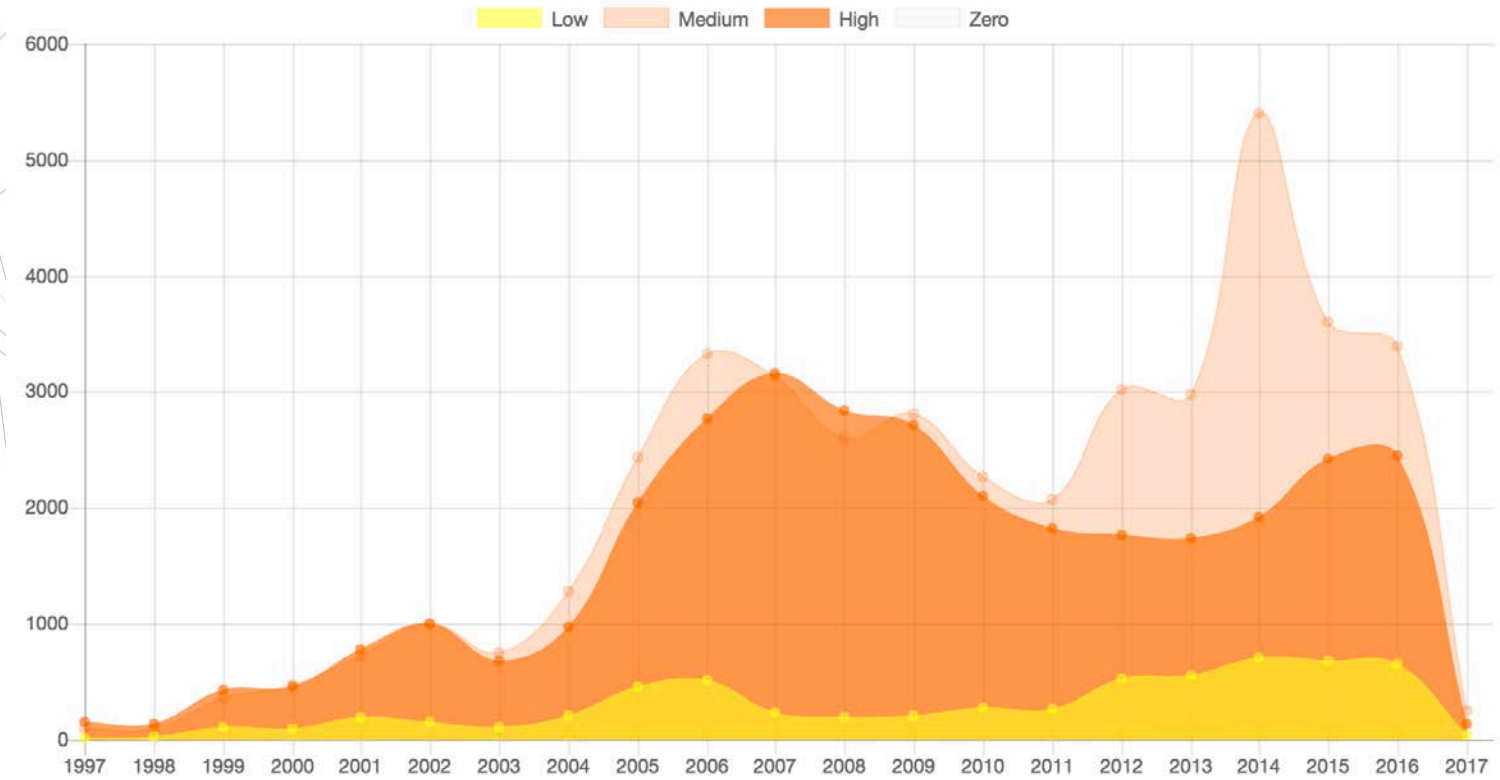
Кирилл Ермаков

IX Уральский форум

2017

#сказочноебанное

Угрозы и уязвимости



Информационный обмен

Процессы выполнения основных задач Центра

Инфор-мационный обмен + Мониторинг ресурсов = Данные об атаках и уязвимостях

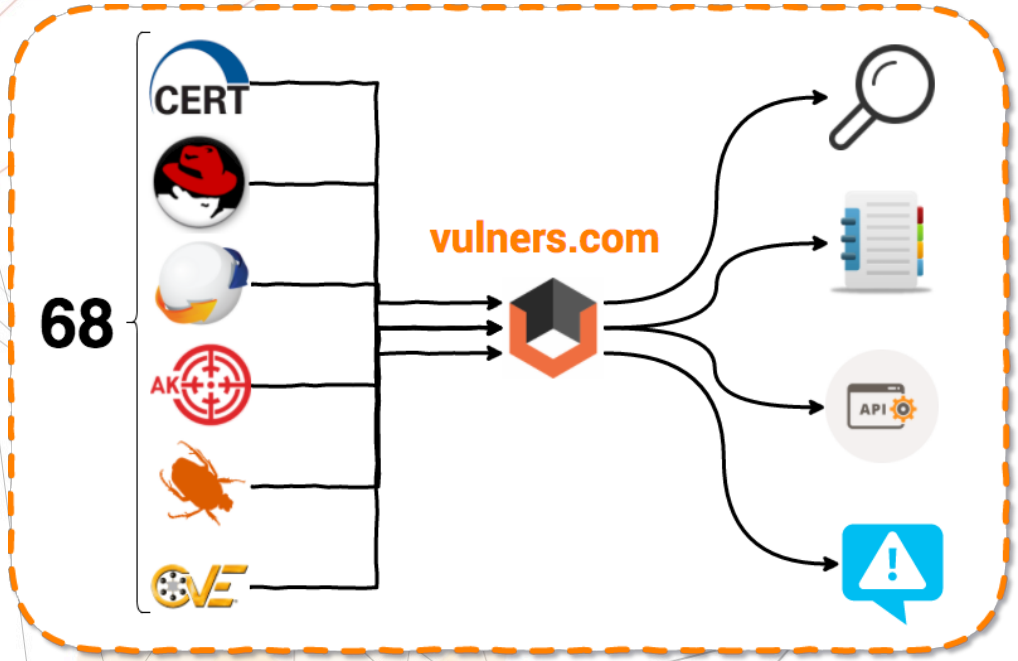
Анализ и обработка данных

- Взаимодействие с правоохранительными органами
- Установление рекомендаций в области обеспечения защиты информации и разработка оперативных рекомендаций
- Формирование аналитических и отчетных материалов

- DDOS атаки
- Вредоносное ПО
- Мошеннические СМС/ звонки
- НСД к конфиденциальной информации

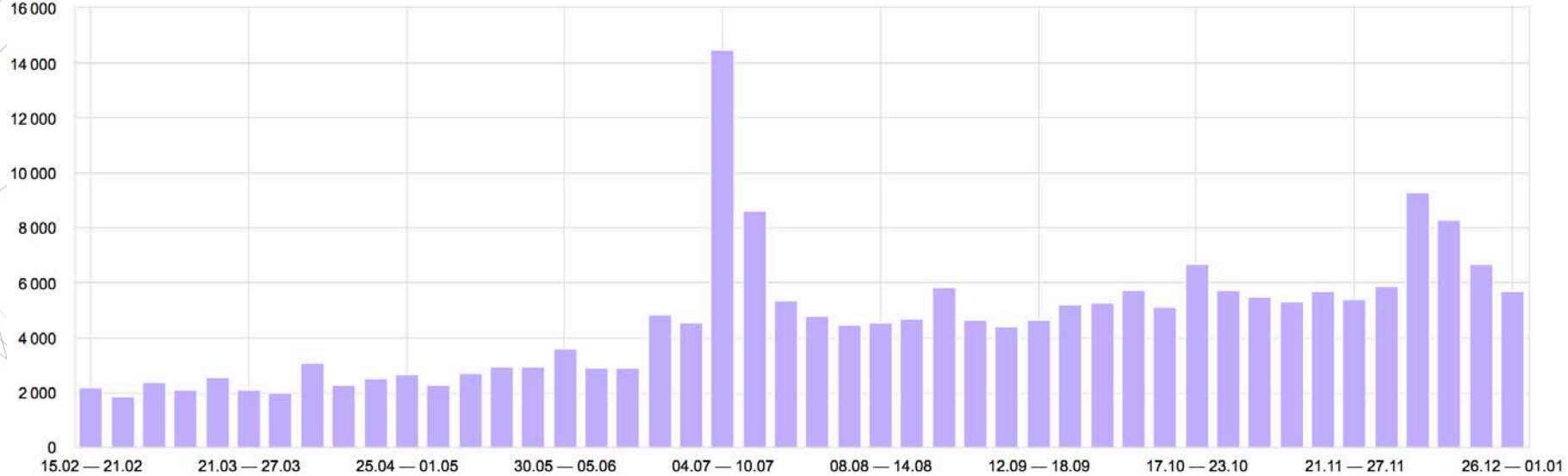
Единая среда обмена информацией об актуальных уязвимостях и атаках

База данных Vulners



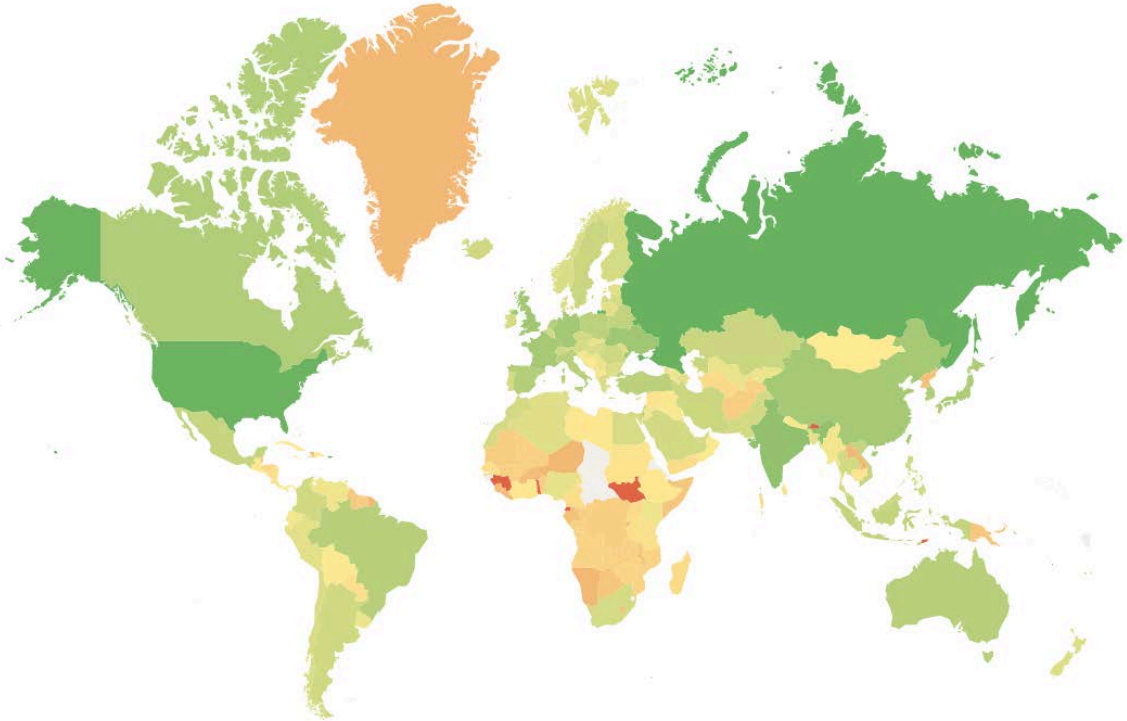
- Одна из крупнейших в мире
- Поисковый движок
- Больше 600,000 бюллетеней безопасности
- 68 источников данных

Посещаемость



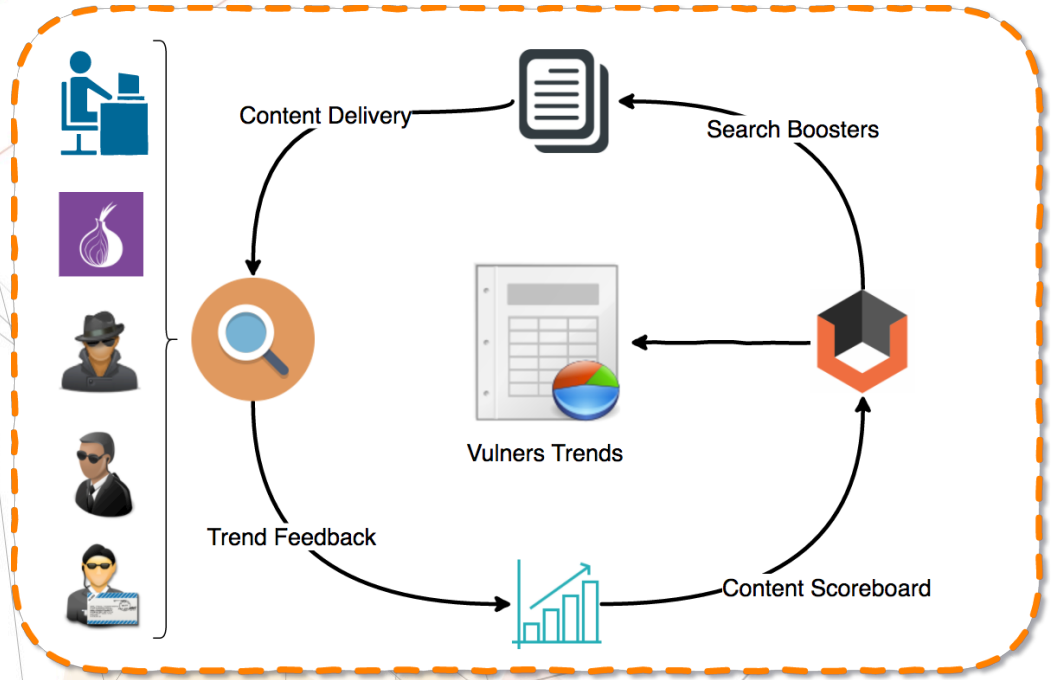
- ±6000 сессий в день
- 52% переходы из поисковиков
- 27,9% прямые заходы

Кто наши пользователи?



- 22,5% Россия
- 19,9% США
- 7% Индия

Система с замкнутым циклом

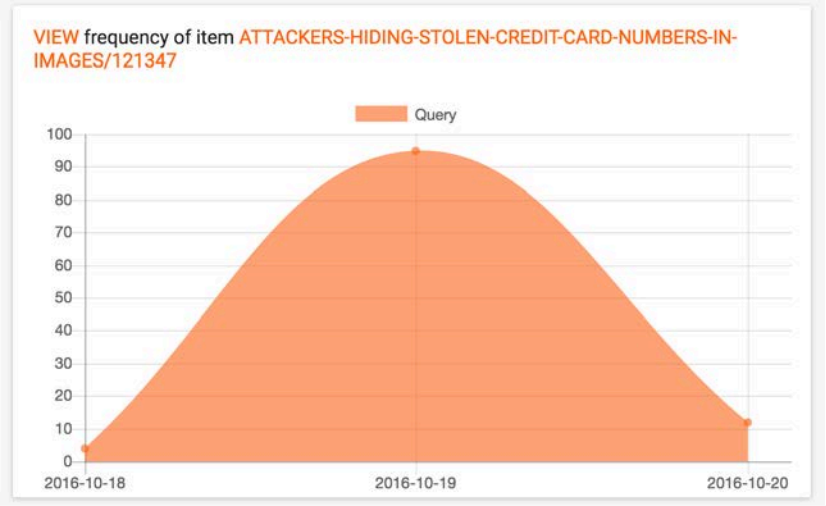


- Релевантность выдачи
- Обратная связь с поиском
- Внутренний рейтинг контента

Ну и зачем это все?

- Скоро все объясню
- Еше 2 слайда теории
- Полчаса до кофе-паузы

Статистические аномалии



Attackers Hiding Stolen Credit Card Numbers in Images
2016-10-18T16:14:00

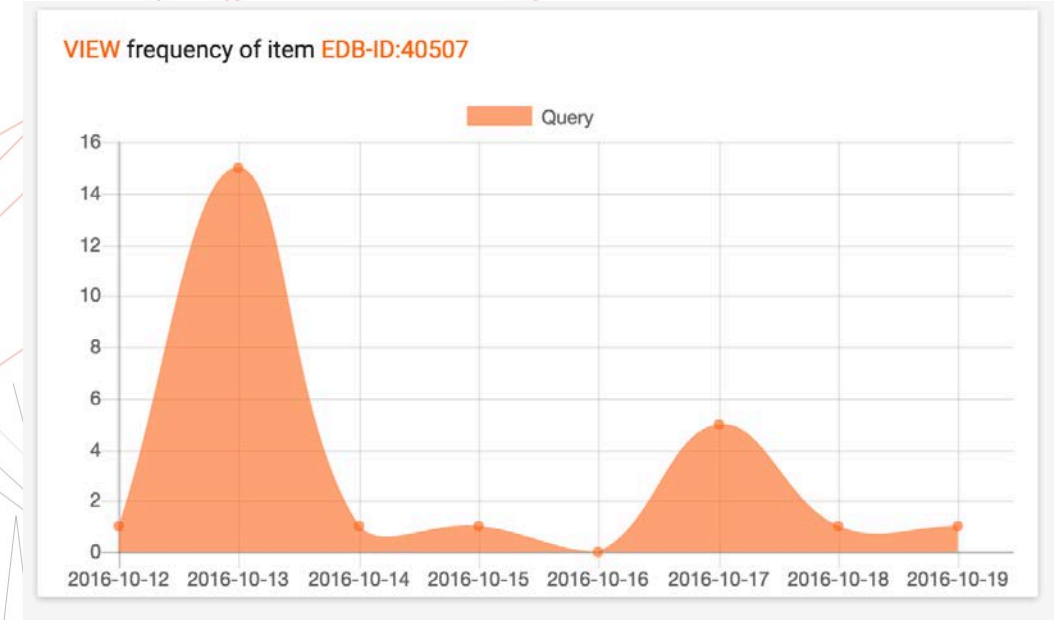
ID ATTACKERS-HIDING-STOLEN-CREDIT-CARD-NUMBERS-IN-IMAGES/121347
Type threatpost
Reporter Chris Brook

Description

Researchers are encouraging developers who use Magento to remain vigilant about securely configuring tl
embedding credit card swipers in sites running the open source e-commerce platform.

- Частотный анализ
- Действительно важные новости
- Внезапный скачок популярности

Корреляции



- Эксплойты к старым уязвимостям
- «И тут внезапно»
- Нарушение стандартного фона

Subversion 1.6.6 / 1.6.12 - Code Execution
2016-10-12T00:00:00

ID EDB-ID:40507
Type exploitdb
Reporter GlacierZ0ne

Description

Subversion 1.6.6 / 1.6.12 - Code Execution. CVE-2013-2088. Remote exploit for Linux platform

```
#  This is an exploit for the subversion vulnerability published as CVE-2013-2088.
#  Author: GlacierZ0ne (kai@ktechnologies.de)
```

Анализ уязвимостей от ФинЦЕРТ

Информационная рассылка FinCERT
Банка России

fincert@cbr.ru

Apache Httpd < 2.4.23: TLS/SSL X.509 client certificate auth bypass with HTTP/2

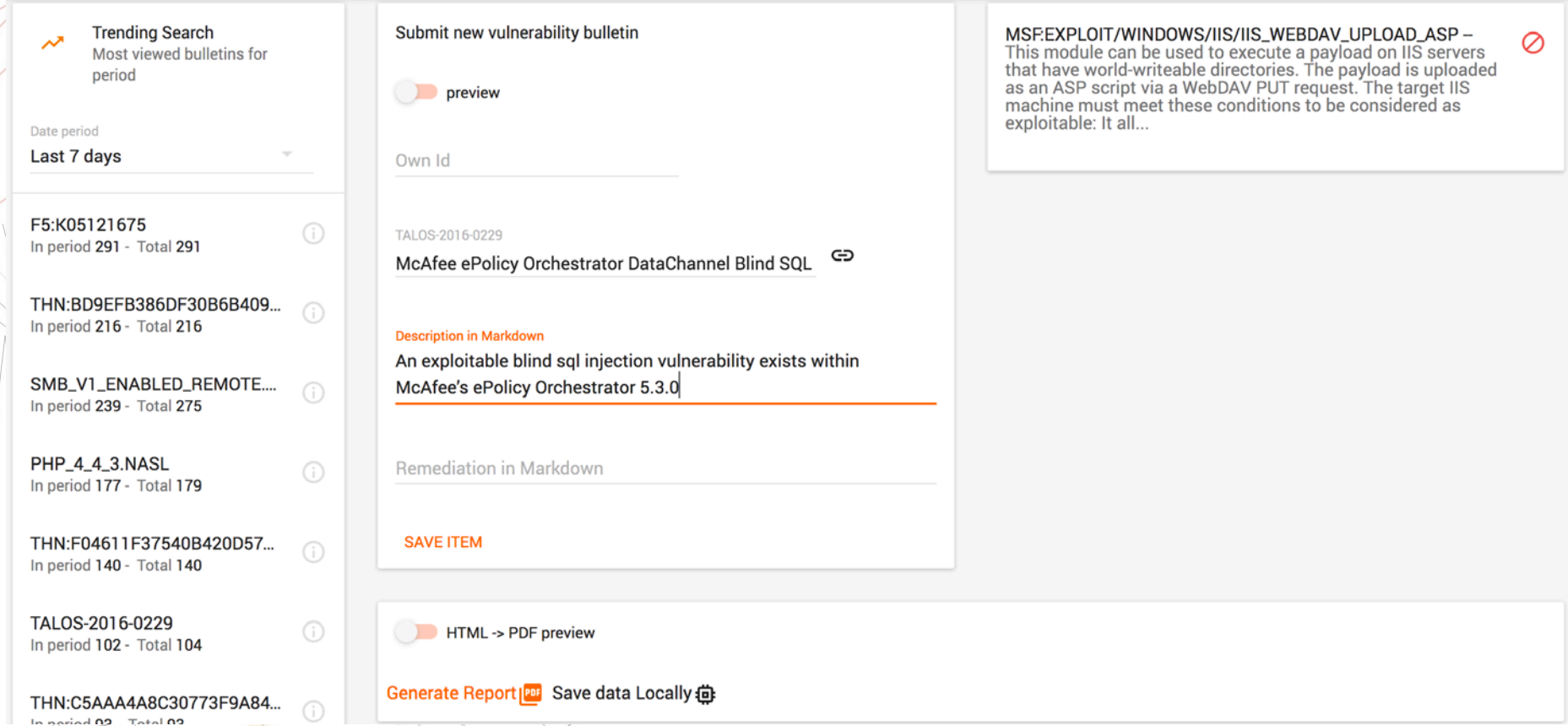
FinCERT ID	HW-Vuln:WEB-Apache-20170127-001
ID	HTTPD:A5459AF02C9EC35CE80EA173C36C3F47
Описание угрозы	Некоторые конфигурации Apache с поддержкой HTTP/2 не проводят проверку сертификата клиента X.509, поскольку "по умолчанию" она не сконфигурирована. Как следствие, возможен несанкционированный доступ к системе к ресурсам, защищаемым через HTTP/2. Ошибка характерна для релизов 2.4.18 и 2.4.20.
Рекомендации	Проверить и исправить при необходимости конфигурацию, включив проверку X.509 или обновить Apache.
Дата публикации	2016-07-05T00:00:00
Ссылки на источник	https://vulners.com/httpd/HTTPD:A5459AF02C9EC35CE80EA173C36C3F47

CVE-2016-7117

FinCERT ID	HW-Vul:OS-LinuxKernelBug-20170127-002
ID	CVE-2016-7117
Описание угрозы	Опасная ошибка в ядре Linux до версии 4.5.2 позволяет удаленному атакующему выполнить код, используя системный вызов recvmmsg .
Рекомендации	Провести обновление системы

- Специальный интерфейс на Vulners
- Генерация PDF/HTML
- Информация о трендах

Взгляд изнутри



Спасибо!

- isox@vulners.com

- Давайте вместе делать мир безопаснее

PS:
Stop paying for features available for free