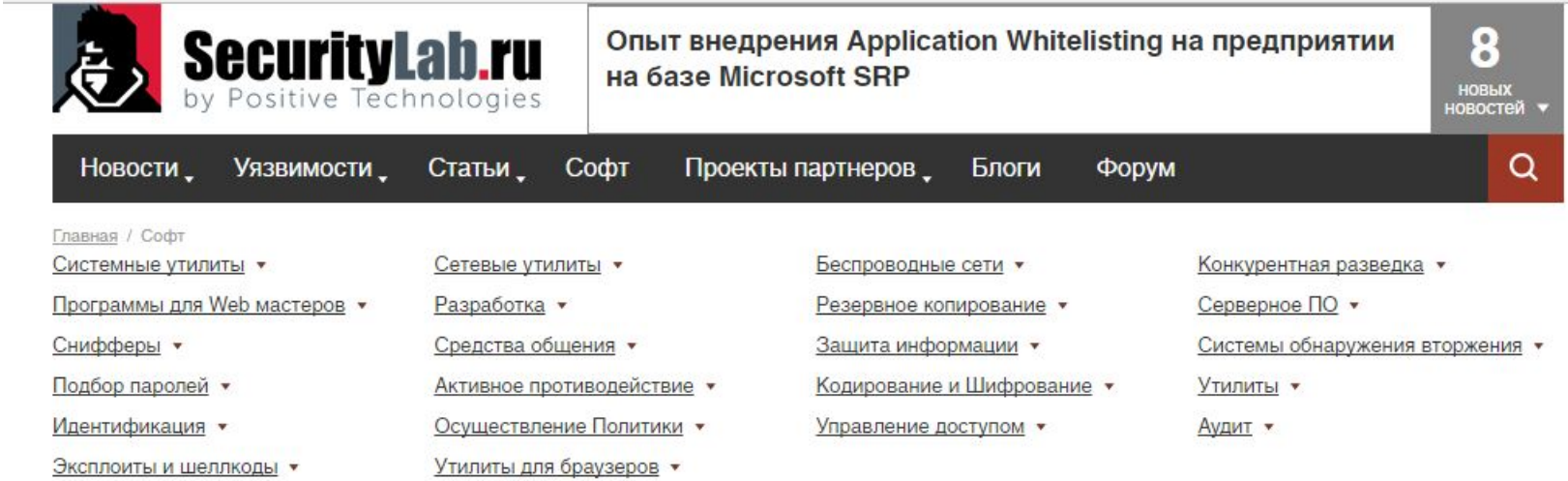
Лаборатория SecurityLab, база уязвимостей

Презентацию подготовил: Федоров В.Ю
Студент группы: ИЭоз-43-21

Что из себя представляет « Лаборатория SecurityLab, база уязвимостей »

Одна из известных российских интернет-порталов,

посвященных проблемам информационной безопасности



Уязвимость PT-2021-07

PT-2021-07: Использование недостатков пары GPay/MasterCard для клонирования транзакций и совершения платежей выше лимитов Tap & Go

Рейтинг опасности:	Средний (5.3) CVSS: 3.0/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
Статус:	Исправление отсутствует
Дата исправления:	
Вектор:	Локальный
Производитель:	MasterCard
ПО:	MasterCard Tokenisation Service (MDES)
Идентификатор:	PT-2021-07
CVE ID:	N/A

Уязвимость обнаружена: Тимур Юнусов (Эксперт)

POSITIVE TECHNOLOGIES

Подробное описание уязвимости

Уязвимое ПО

MasterCard Tokenisation Service (MDES)

Рейтинг опасности

Уровень опасности: Средний
Использование недостатков пары GPay/MasterCard для клонирования транзакций и совершения платежей выше лимитов Tap & Go
Вектор атаки: Локальный

CVSS v3.0
Base Score: 5.3
Vector: (AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N)

Описание уязвимости

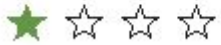
GPay позволяет использовать режим MasterCard M/STRIPE с низкой энтропией 1000, уязвимый к атаке на клонирование криптограмм. Злоумышленник может создать функциональный клон мобильного кошелька GPay и совершать платежи выше лимитов Tap & Go в магазинах по всему миру. В случае использования GPay в странах Евросоюза, злоумышленник может склонировать только 5 транзакций, что гарантирует ему шанс на успешное совершение операции 22% в случае совершения 50 попыток.

Статус уведомления

10.2021 - Производителю отправлены детали уязвимостей

Разделение на уровень опасности

Рейтинг опасности:



Низкая

Рейтинг опасности:

Средняя

Рейтинг опасности:

Высокая

Рейтинг опасности:

Очень высокая

КОНЕЦ