

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

The screenshot shows the top section of the SecurityLab.ru website. On the left is the logo, which consists of a stylized shield with a keyhole and a padlock, next to the text "SecurityLab.ru by Positive Technologies". To the right of the logo is a main headline: "Опыт внедрения Application Whitelisting на предприятии на базе Microsoft SRP". Further right is a grey box with the number "8" and the text "НОВЫХ НОВОСТЕЙ" with a dropdown arrow. Below these elements is a dark navigation bar with the following items: "Новости", "Уязвимости", "Статьи", "Софт", "Проекты партнеров", "Блоги", "Форум", and a search icon. Below the navigation bar is a grid of category links, each with a dropdown arrow:

- Главная / Софт
- Системные утилиты
- Программы для Web мастеров
- Снифферы
- Подбор паролей
- Идентификация
- Эксплоиты и шеллкоды
- Сетевые утилиты
- Разработка
- Средства общения
- Активное противодействие
- Осуществление Политики
- Утилиты для браузеров
- Беспроводные сети
- Резервное копирование
- Защита информации
- Кодирование и Шифрование
- Управление доступом
- Конкурентная разведка
- Серверное ПО
- Системы обнаружения вторжения
- Утилиты
- Аудит

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:N/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

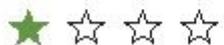
GPay позволяет использовать режим MasterCard M/STRIPE с низкой энтропией 1000, уязвимый к атаке на клонирование криптограмм. Злоумышленник может создать функциональный клон мобильного кошелька GPay и совершать платежи выше лимитов Tap & Go в магазинах по всему миру. В случае использования GPay в странах Евросоюза, злоумышленник может клонировать 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

Средняя

Рейтинг опасности:



Высокая

Очень высокая

Рейтинг опасности:



Рейтинг опасности:



КОНЕЦ

