
ВЗЛОМ И ЗАЩИТА ОКРУЖАЮЩЕГО МИРА
BEHOLDER
IS
HERE
2022

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

1. Видеонаблюдение

BEHOLDER
IS
HERE

исследования и консалтинг

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Видеонаблюдение/ РИСКИ

- Вывод из строя
- Дистанционное наблюдения
- Манипулирование видео потоком
- Изменение/удаление архива
- Вектор сетевой атаки

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Видеонаблюдение/ ПРОБЛЕМЫ

Типовые OEM платформы

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Видеонаблюдение/ ПРОБЛЕМЫ

Стандартные пароли к оборудованию

- ACTi: admin/123456 or Admin/123456
- Arecont Vision: none
- Avigilon: Previously admin/admin, изменен Administrator/ в более старых версиях прошивки
- Axis: Стандартно root/pass, но новые камеры Axis предлагают создать пароль при первом входе в систему (внимание, root/pass можно применять для доступа ONVIF, но для входа в камеру требуется создания пароля root)
- Basler: admin/admin
- Bosch: Не требует, но новые версии прошивки (6.0+) предлагают создать универсальный пароль при первом запуске системы.
- Brickcom: admin/admin
- Canon: root/camera
- Cisco: Нет заводского пароля, предлагает создать при первом запуске системы.
- Dahua: Просит создать пароль при первом запуске системы. Ранее этот процесс был рекомендацией, но его можно было отменить; в старых моделях заводской пароль admin/admin
- Digital Watchdog: admin/admin
- FLIR: admin/fliradmin
- FLIR (Dahua OEM): admin/admin
- FLIR (Quasar/Ariel): admin/admin
- Foscam: admin/
- GeoVision: admin/admin
- Grandstream: admin/admin
- Hanwha: admin/заводского пароля нет, необходимо создавать во время первой настройки.
- Hikvision: Прошивка 5.3.0 и выше просит создать уникальный пароль; ранее admin/12345
- Honeywell: admin/1234
- IndigoVision (Ultra): нет
- indigoVision (BX/GX): Admin/1234
- Intellio: admin/admin
- IPX-DDK: root/admin или root/Admin
- JVC: admin/jvc
- Longse: admin/12345
- Lorex: admin/admin
- LTS: Просит создание уникального пароля; ранее admin/12345
- March Networks: admin/
- Mobotix: admin/meinsm
- Northern: Прошивка версии 5.3.0 и выше требует создания уникального пароля; ранее; ранее admin/12345
- Oncam: admin/admin
- Panasonic: Прошивка версии 2.40 и выше требует создания имени пользователя и пароля; ранее admin/12345

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

GoAhead webserver

Auth bypass & Root RCE

~1250 моделей камер и регистраторов

>185 тысяч уязвимых публичных устройств

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Видеонаблюдение/ ПРОБЛЕМЫ

Обслуживание и обновления

- Медленная реакция OEM производителя и ооооочень медленная у вендора на уязвимости
- Сложный организационный процесс на объекте
- Недостатки при проектирование.
- «Работает же! И так сойдет!!!»

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

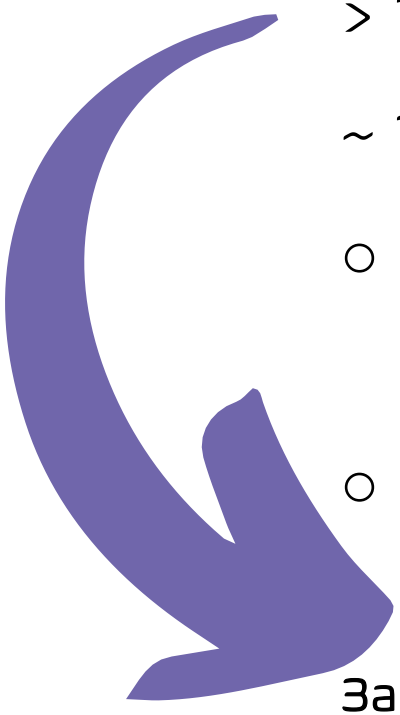
Видеонаблюдение/ УГРОЗЫ

- Сброс пароля «по умолчанию»
- Обход пароля и получение root привилегий
- Доступ к видео потоку без авторизации
- Доступ к конфигурированию устройства без авторизации
- Загрузка модифицированных прошивок

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Видеонаблюдение/ УГРОЗЫ/ ПРИМЕРЫ

DAHUA BACKDOOR. GENERATION 2&3



> 1140000 устройств

~ 1000 моделей OEM IPC / DVR / NVR

- Загружает пользовательскую базу данных со всеми учетными данными и правами доступа.
- Добавляет/изменяет/удаляет любого пользователя

Закрытие уязвимости в прошивках DAHUA – март 2017

Закрытие уязвимости в прошивках OEM вендоров - ?

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Видеонаблюдение/ УГРОЗЫ/ ПРИМЕРЫ

HIKVISION BACKDOORS

- Удаленный сброс пароля
- Обращение к HikCGI API (без авторизации)
- Статичный ключ шифрования (ABCDEFG)
- Встроенный рабочий WIFI модуль без авторизации.
- Отсутствие защиты от Брутфорса

Закрытие уязвимости в прошивках HIKVISION – ноябрь 2017

Закрытие уязвимости в прошивках OEM вендоров - ?

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Видеонаблюдение/ ЗАЩИТА

- Меняем стандартные логины и пароли
- Постоянно обновляем прошивки
- Включаем принудительную авторизацию
- Создаем отдельные сети VLAN и защищаем сеть
- Фильтрация IP адресов
- Отключаем камеры от сторонних встроенных сервисов.
- Закрываем неиспользуемые порты и сервисы
- Контроль активности сетевого окружения
- Включаем OSD меню на камерах

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

2. Охранная сигнализация

BEHOLDER
IS
HERE

исследования и консалтинг

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

ОХРАННАЯ СИГНАЛИЗАЦИЯ/ РИСКИ

- Вывод из строя
- Отключение
- Перехват управление.

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОХРАННАЯ СИГНАЛИЗАЦИЯ/ ПРОБЛЕМЫ

- Незашифрованный передаваемые данные между устройствами
- Возможность глушения беспроводных интерфейсов
- Некачественная компонентная база

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОХРАННАЯ СИГНАЛИЗАЦИЯ/ УГРОЗЫ

- Воспроизведение команды
- Подбор посылок
- «Отказ от обслуживания»
- Клонирование
- Глушение
- Spoofing
- Sniffing

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОХРАННАЯ СИГНАЛИЗАЦИЯ/ УГРОЗЫ

- Правильное проектирование
- Правильный подбор оборудования
- Тестирование на проникновение
- Пост- инсталляционная настройка
- Тревога на глушение

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

3. СКУД

BEHOLDER
IS
HERE

исследования и консалтинг

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

СКУД/ РИСКИ

- Неавторизированный доступ
- Перехват идентификационной информации

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

СКУД/ ПРОБЛЕМЫ

- Использование простых идентификаторов
- Переоцененность биометрических данных
- Отсутствие регламентов выдачи временных пропусков
- Отсутствие контроля соответствия

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

СКУД/ УГРОЗЫ

- Копирование технических идентификаторов
- Копирование биометрических идентификаторов

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

СКУД/ УГРОЗЫ

- Копирование технических идентификаторов
- Копирование биометрических идентификаторов
- Доступ к базе данных СКУД

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

СКУД/ Защита

- Использование криптостойких технических идентификаторов
- Использование многофакторной аутотентификации
- Правильная организация работы бюро пропусков
- Ограничение по времени работы пропусков
- Запрет повторного прохода
- Визуальный контроль

СПАСИБО ЗА ВНИМАНИЕ!
ВОПРОСЫ?

T.ME/ForensicTools

СПАСИБО ЗА ВНИМАНИЕ!
ВОПРОСЫ?

T.ME/BEHOLDERISHERE