EBU

OPERATING EUROVISION AND EURORADIO

R 142

CYBERSECURITY BEST PRACTICES FOR CONNECTED TELEVISIONS AND SERVICES

RECOMMENDATION

Geneva
April 2016

EBU

OPERATING EUROVISION AND EURORADIO

R 142

CYBERSECURITY BEST PRACTICES FOR CONNECTED TELEVISIONS AND SERVICES

RECOMMENDATION

Внимание!
Данный перевод **НЕ** претендует на аутентичность
и может содержать отдельные неточности.
Оригинал документа на сайте https://tech.ebu.ch

ПЕРЕДОВАЯ ПРАКТИКА КИБЕРБЕЗОПАСНОСТИ ДЛЯ ПОДКЛЮЧЕННЫХ К ИНТЕРНЕТУ ТЕЛЕВИЗОРОВ И УСЛУГ

РЕКОМЕНДАЦИЯ

Женева
Апрель 2016

Передовая практика безопасности для подключенных к интернету телевизоров и услуг

Комитет EBU	*Первый выпуск*	*Переработка*	*Переиздание*
TC	2016		

Ключевые слова: SMART TV, Connected TV, HbbTV, Услуга, Безопасность, Корневой сертификат, «Игра в песочнице».

Рекомендация

EBU, учитывая, что

1. Медиа компании все чаще предоставляют услуги HbbTV, доступные через бытовые телевизоры.
2. Киберугрозы вредоносных программ становятся проще в исполнении.
3. Подключенные медиа устройства и телевизоры в частности имеют очень низкий порог безопасности, унаследованный с эпохи неподключенных вещательных медиа
4. Обнаружившиеся уязвимости подключенных телевизоров могут повредить репутации производителей телевизоров и поставщиков услуг.

Рекомендует вещателям и поставщикам ТВ услуг с подключением к интернету:

1. Использовать безопасные протоколы (например, http) по необходимости для целостности и конфиденциальности ТВ услуг с подключением к интернету.
2. Использовать корневые сертификаты TLS для услуг HbbTV, как описано в [1].

EBU также рекомендует в подключенных телевизорах:

3. Если веб-сайты используют для передачи http, устройство не должно принимать сертификаты из ненадежных корневых каталогов. Для приложений HbbTV список корневых сертификатов TLS, которые должны поддерживаться терминалами HbbTV, можно найти в [1]. То же применимо к выполнению скриптового кода (например, JavaScript) в веб-браузере или браузере HbbTV.
4. Процессы должны быть разделены (функции, которые могут выполняться с кнопки удаленного контроллера, должны работать отдельно от системных процессов, например, браузера).
5. Процессы с выходом в интернет всегда должны работать без привилегий (некорневые аккаунты).
6. Неиспользуемые или ненужные сервисы должны отключаться или деактивироваться по умолчанию.
7. Все зоны операционных систем должны быть корректируемы и регулярно корректироваться. Для старых устройств, которые уже не поддерживаются производителем, должны быть четкие сообщения о том, что патчей для этих старых телевизоров уже нет. Для всех подключенных телевизоров необходима поддержка минимум на 5 лет.
8. Должны быть установлены антивредоносные технологии.
9. Необходимы регулярные проверки операционной системы и приложений поставщика для идентификации уязвимостей и дефектов, особенно перед выпуском финальной версии.
10. Перезагрузка прошивки должна перезагружать все устройство, включая все файловые системы.
11. Операционная система должна быть защищена посредством передовой практики. По возможности следует интегрировать технологии обязательного контроля доступа (MAC), например, SELinux.
12. Веб-браузер (веб-браузер и/или приложение веб-браузера) должен использовать современные механизмы защиты веб-браузера, например:
    a. «Игра в песочнице» (для веб-сайтов и плагинов).
    b. Безопасная обработка cookie.
    c. Антишпионские технологии, например, ASLR, DEP, SEH.
    d. Антивредоносные технологии, например, защита от вредоносных веб-сайтов.

Ссылки

[1] http://dtg.org.uk/work/DBook_Resources/dtgrootcert.html