



Обзор возможностей, настройка и рекомендации по безопасности для веб-сервера Windows CE

Станислав Павлов
Системный аналитик
Кварта Технологии



Содержание

- Обзор веб-сервера Windows CE
- Безопасность сервера
- Серверные скрипты

Зачем нам нужен веб-сервер на CE устройстве?

- Интерфейс пользователя для автономных устройств
 - Домашний шлюз
 - Файл-сервер
 - Торговый автомат
- Интерфейс для более высокоуровневых протоколов
 - UPnP
 - SOAP
 - MSMQ Web Messaging

Брат IIS

- **Windows CE Web Server – это не порт IIS**
- **Аналогично IIS**
 - **Расширения ISAPI**
 - **Фильтры ISAPI**
 - **Поддержка подмножества ASP**
 - **Инструментарий SOAP/UPnP**

Младший брат IIS

Не конкурент IIS

- Только 110 KB памяти ROM для ядра
- Полностью, для X86 процессора, с поддержкой ASP - 1.8 Мб
- Не масштабируется – максимум 10 соединений по умолчанию
- Нет метаданных – вся конфигурация в реестре
- Нет ASP .NET

Виртуальные корневые каталоги

- Виртуальные корневые каталоги (vroots) отображают запрашиваемые URL в физические пути на устройстве
 - <http://WinCE/foo> отображается в \windows
 - <http://WinCE/bar> отображается в \temp
- Настраивается в реестре
- Удобно для организации веб-сайта и ограничения доступа к определенным таблицам

Несколько веб-сайтов

- Веб-сайт – это набор конфигурационных настроек (главным образом vroots)
- Веб-сайт определяется сетевым интерфейсом, используемом для приема запросов HTTP
- Сценарий домашнего шлюза
 - Страницы конфигурации доступны только с компьютеров из приватной сети
 - Защищает пользователей от случайного размещения приватной информации в интернете

Журналирование запросов

- По умолчанию веб-сервер журналирует все HTTP запросы
- Пример записей в журнале
 - Fri, 07 May 2004 19:47:53 10.0.0.5 GET /WebAdmin 200
 - Fri, 07 May 2004 19:47:56 10.0.0.5 POST /WebAdmin 200
- Журналирование использует простой механизм перезаписи для защиты от переполнения устройства журналом
 - Сначала текущий - httpd.log, затем предыдущий - httpd.log
- Максимальный размер и директория настраиваются
 - По умолчанию 32KB и \windows
- Удобно для отладки и детектирования атак

Удаленный доступ к файлам WebDAV

- Веб-сервер поддерживает WebDAV (RFC2518)
- WebDAV позволяет модифицировать, создавать и удалять файлы на удаленном устройстве по HTTP каналу
- WebDAV интегрирован в редиректор файловой системы Windows XP
 - Можно отобразить виртуальный каталог Windows CE HTTP как диск XP
 - `net use * http://WinCE/Foo`

Содержание

- Обзор веб-сервера Windows CE
- Безопасность сервера
- Серверные скрипты

Безопасность веб-сервера

- Это очень важно. Неверно сконфигурированный веб-сервер, может позволить злоумышленникам
 - Просматривать любые файлы на устройстве
 - Сломать устройство
 - Запускать конфигурационные программы (напр. WebAdmin), которые дают им полный контроль за устройством
 - Загружать свои собственные серверные скрипты на устройство (Троянские программы)
- Вы должны очень тщательно конфигурировать настройки безопасности

Максимальная безопасность по умолчанию

- Microsoft поставляет веб-сервер Windows CE сконфигурированный максимально безопасно по умолчанию
 - По умолчанию ни один серверный скрипт не ставится с веб-сервером
 - Если серверные скрипты вручную добавляются (напр. WebAdmin), доступ к ним требует аутентификации
 - На шлюзе – защитный экран (Firewall) по умолчанию
 - Нет доступа к веб-сайту, если на шлюзе отключен защитный экран
- Вы *все равно* должны тщательно настраивать безопасность

Аутентификация пользователей

- Аутентификация настраивается для виртуального корневого каталога
- Поддерживается два типа аутентификации
 - Basic – пароль открытым текстом
 - NTLM – Internet Explorer и Netscape 7.1
- Откуда CE берет имена/пароли пользователей для проверки?
 - Локальная база пользователей на устройстве (NTLMSetUserInfo и соответствующий API)
 - или –
 - Контроллер домена Windows указанный в реестре

Список пользователей

- **Защититься просто паролем – недостаточно в большинстве случаев**
 - **Вася Пупкин не должен иметь доступа к WebAdmin, но должен иметь возможность просматривать картинки**
- **Виртуальные корневые каталоги могут разрешать или запрещать доступ пользователям или группам пользователей**
 - **На практике, большинство устройств CE имеют одного пользователя (Admin), но нужно чтобы было не так ...**
- **Пример формата списка пользователей**
 - **John; -Bob; @Developers; -@ProgramManagers;***

Права пользователей

- Помимо аутентификации пользователя на виртуальную корневую папку, могут быть настроены дополнительные ограничения
- Виртуальные корневые каталоги могут предоставлять или запрещать
 - Чтение (получение «сырого» содержимого файла)
 - Исполнять (запускать расширения ISAPI)
 - Писать (загрузка файлов через WebDAV)
 - Скрипт (запуск ASP страниц)
 - Исходные коды скриптов (просмотр исходного кода для ASP/ISAPI)
- Флаги `HSE_URL_FLAGS_XXX` в `httpext.h`

Безопасные соединения

- Веб-сервер поддерживает Secure Socket Layer (SSL) для шифрования данных
- Требуется сертификат сервера на устройстве CE
- Клиент должен аутентифицировать сервер
 - Нет обходного пути!
 - Сервер должен доказать, что его адрес не был подменен
- Трудно настроить практически
 - Необходим сертификат сервера, подписанный доверенным уполномоченным (trusted authority)

Безопасность: советы

- Добавляйте в образ только те компоненты, которые вам абсолютно точно нужны
- Понимайте, что вы добавляете в образ
- Для шлюзов – используйте фаервол
- Для публично доступных сайтов – минимальные привелегии
- Требуйте аутентификации
- Будьте *экстремально* внимательны, когда разрабатываете собственные серверные скрипты

Содержание

- Обзор веб-сервера Windows CE
- Безопасность веб-сервера
- Серверные скрипты

Серверные скрипты «выравнивают» барьеры безопасности!

- Как Windows CE веб-сервер предоставляет интерфейс пользователя для домашних шлюзов, торговых автоматов и т.д.?
- Эксперт (ВЫ) пишет код, который вызывается веб-сервером, для отображения вашего приложения
- Три опции в CE
 - Фильтры ISAPI
 - Расширения ISAPI
 - Страницы ASP

ISAPI фильтры – максимальная сила

- Фильтры ISAPI вызываются веб-сервером на различных стадиях работы с веб
 - Чтение/отсылка «сырых» данных
 - Разбор полей HTTP
 - Отображение URL на виртуальный корневые папки
 - и т.д. ...
- Фильтры получают информацию о HTTP запросе и могут модифицировать ее «посередине»
 - Пример: Фильтр может перезаписать трансляцию виртуальных папок веб-сервера

ISAPI фильтры – слишком сильно?

- Как для IIS, так и для Windows CE может быть сложно заставить работать ISAPI фильтр, как необходимо
- Изменение «сырых» HTTP потоков (как входящих так и исходящих) не приветствуется в Windows CE
- Перед написанием, будьте абсолютно уверены, что нет альтернативы
 - Почему бы не сделать это используя расширения ISAPI и/или настройки веб-сервера

ISAPI расширения – хлеб с маслом разработки CE

- Все веб-сервисы в Windows CE Core OS реализованы как расширения ISAPI
 - WebAdmin/RemoteAdmin/другой ИП
 - SOAP
 - UPnP
 - MSMQ Web Messaging
- Почему?
 - Гораздо меньшие накладные расходы чем при использовании ASP страниц
 - Понятный процесс разработки

ISAPI расширения - Реализация

- Реализуются как библиотека DLL экспортирующая три функции
 - `GetExtensionVersion` – вызывается загрузке
 - `HttpExtensionProc` – вызывается при обработке веб-запроса
 - `TerminateExtension` – вызывается при выгрузке
- Расширение вызывается когда виртуальный путь отобразит запрос HTTP на физический путь
- Очень похоже на реализацию для IIS
 - Просто портировать

HttpExtensionProc – Часть 1

- Вызывается веб-сервером один раз на запрос
- Получает один аргумент – структуру `LPEXTENSION_CONTROL_BLOCK`
- Структура содержит данные доступные только для чтения
 - Длину запроса POST
 - До 48Кб данных POST
 - Строку запроса
 - Content Type

HttpExtensionProc – Часть 2

- **LPEXTENSION_CONTROL_BLOCK** также содержит ссылки на функции обратного вызова веб-сервера
 - **GetServerVariable** – получение информации о запросе HTTP
 - Посланные Cookies, IP адрес клиента, и т.д.
 - **WriteClient** – посыл данных напрямую клиенту через HTTP поток
 - **ReadClient** – чтение дополнительной POST информации (если длинна присланного больше 48 Кб)
 - **ServerSupportFunction** – другие доступные функции сервера

Пример расширения ISAPI

Использование: <http://WinCE/Simple.dll?John>

```
HttpExtensionProc(LPEXTENSION_CONTROL_BLOCK p)
{
    CHAR szBuf[MAX_PATH];
    DWORD dwLen = sprintf(szBuf, "Hello user <%s>", p->lpszQueryString);
    p->WriteClient(pECB->ConnID, szBuf, &dwLen, 0);
    return HSE_STATUS_SUCCESS;
}
```

Вывод: Hello user <John>

Я должен быть уволен за написание такого кода. Почему?

Больше безопасности!

- Эта строчка кода непростительна даже в примере из 4-х строчек
 - `printf(szBuf, "Hello user <%s>", p->lpszQueryString);`
- Веб-сервер ни дает никаких гарантий, что длинна строки `lpszQueryString < MAX_PATH`
- Если длинна строки `> MAX_PATH`, то переполнение буфера. Это может быть использовано хакерами.

Выученные уроки безопасности

- **НИЧЕМУ НЕ ВЕРЬТЕ!**
- **Веб-сервер скрывает детали HTTP, но это не означает, что вы не должны проверять данные**
- **Веб-сервер работает в services.exe, который является доверенным процессом. Если хакер «сломает» ваше ISAPI, он завладеет устройством**
- **Зачем вообще позволять неизвестным пользователям иметь доступ к вашим расширениям ISAPI? Используйте аутентификацию веб-сервера как первую линию обороны**

Упрощение процесса разработки

- Windows CE Core Team использует общие вспомогательные классы, для упрощения написания ISAPI
 - Автоматически поддерживает keep-alive
 - Упрощает разбор “реальных” строк запроса/данных POST
- Код доступен в Platform Builder
 - `\PUBLIC\SERVERS\OAK\SAMPLES\NATADMIN\BASEISAPI`

ASP – Еще проще

- **Active Server Pages (ASP) – это смесь HTML и кода VBScript/JScript**
- **Код обрабатывается сервером**
- **ASP предоставляет экстремально мощную объектную модель**
- **Нет необходимости писать на C/C++ (для простых страниц 😊)**

Простой синтаксис ASP

- Напишите HTML, который по умолчанию напрямую шлетя пользователю
- `<% и %>` - тэги ограничивающие скрипт
- Расположите скриптовый код между этими тэгами, чтобы он исполнялся на сервере
- Базовые объекты ASP
 - Request – получает информацию о запросе HTTP
 - Response – строит HTTP ответ

Пример ASP

Ввод: <http://WinCE/simple.asp?FN=John&LN=Spaith>

```
<%@ LANGUAGE=JSCRIPT %>
<% var prefix = "";
    var last = Request.QueryString("LN");
    if (Request.QueryString("FN") == "John")
        prefix = "Mr.";
    if (Request.QueryString("FN") == "Barbara")
        prefix = "Ms.";
%>
Hello, <% Response.Write(prefix + " " + last) %>
```

Вывод: [Hello, Mr. Spaith](#)

ASP и доступ к системе

- Скриптовые языки имеют очень ограниченный доступ к системе, по дизайну
 - Никакого прямого доступа к Win32 API
- Скрипты могут вызывать и работать с COM объектами, которые вы разрабатываете
 - Разместите логику системы в COM объектах, отображение на ASP страницах

Заключение

- Обзор веб-сервера Windows CE
- Безопасность веб-сервера
- Серверные скрипты



Веб-сервер - мощная платформа для разработки приложений, работающих в сети, но необходимо тщательно прорабатывать вопросы сопутствующей безопасности



Вопросы?

Станислав Павлов
Системный аналитик
Кварта Технологии

