**Управление заплатами в ОС Windows**

Марсин Полич (Marcin Policht)

Управление заплатами (patch management, без сомнения, является одной из наиболее критически важных и сложных проблем наших дней, связанных с безопасностью операционных систем Windows. Эта проблема обострилась в последние несколько месяцев из-за увеличения частоты выпуска Microsoft заплат, расцениваемых как «критические», что являлось реакцией компании на злонамеренные программы, использующие возможности основных уязвимостей (для того, чтобы получить полный список заплат, обратитесь к разделу Web-сайта Microsoft, посвященному проблемам безопасности).

Это становится особенно важным, поскольку Microsoft изменила собственную классификацию степени безопасности систем в начале 2003 года, введя категорию «важная» (important) (в дополнение к «критической», «умеренной» и «низкой» категориям), чтобы более точно отражать уровень срочности, который должен приниматься во внимание при развертывании заплат. Благодаря этому, «критическая» оценка резервируется только для уязвимостей, которые могут быть использованы злонамеренными Интернет-червями, распространяющихся без вмешательства пользователей.

Давление со стороны заказчиков, вынуждающее предоставлять аварийное программное обеспечение, развертываемое на сотнях или даже тысячах компьютеров, заставляет Microsoft искать средства для облегчения подобных усилий. Это привело к новому циклу выпуска заплат, появление которого относится к ноябрю 2003 года. В отличие от предыдущего еженедельного расписания (каждая среда), новые заплаты теперь становятся доступными для загрузки во второй вторник каждого месяца (за очевидным исключением для критически важных выпусков). И хотя это изменение упрощает для корпоративных ИТ-подразделений координацию графиков развертывания, им необходимо также выбрать методологию, позволяющую учитывать и устанавливать заплаты на всех управляемых системах Windows с максимальной точностью и скоростью (это особенно важно, поскольку теперь уже очевидно, что даже несколько зараженных червем компьютеров могут серьезно снизить функциональность всей компьютерной сети).

В статьях этой серии предпринимается попытка оценить возможности, доступные в настоящее время, поскольку мы пытаемся упростить процесс выбора. Мы обсудим как бесплатные методы развертывания (основанные на усовершенствованиях в операционных системах Microsoft, инструментах сторонних производителей и решениях, основанных на использовании сценариев), так и продукты, поставляемые на платной основе. Эта первая статья дает обзор разработок в технологиях, связанных с установкой заплат, сделанных за последние несколько лет и обсуждает главные концепции управления заплатами.

Наиболее простым и популярным решением Microsoft по управлению заплатами является инструмент Windows Update, представленный в Windows 2000 (и получивший дальнейшее развитие в Windows XP и 2003). Этот инструмент прост в установке и конфигурировании (особенно после усовершенствований групповых политик (Group Policy, добавленных в Windows XP, основан на агентах (agent, запускаемых на целевых системах и запрашивающих новые заплаты из предварительно определенного расположения (по умолчанию, это группа управляемых Microsoft серверов Windows Update. Windows Update способен обслуживать как отдельных пользователей, так и небольшие предприятия. К сожалению, он не очень хорошо подходит к жестко структурированным корпоративным средам, в которых изменения должны контролироваться более надежно и централизованно. Кроме того, Windows Update был предназначен только для новейших операционных систем, тогда как подавляющая часть настольных систем и серверов продолжала работать под Windows NT 4.0.

Чтобы обеспечить большую избирательность в развертывании заплат и принимая во внимание проблему традиционных операционных систем, Microsoft обратила свое внимание на продукты, поставляемые сторонними разработчиками. Похоже, что эпидемии Code Red и Nimda, вспыхнувшие в сентябре 2001 года, ускорили это решение. Сначала Microsoft обратилась к неотложным нуждам, выпустив утилиту IIS Lockdown для автоматического конфигурирования безопасности Internet Information Server; однако было ясно, что существует потребность для более общих решений по устранению других уязвимостей операционных систем Windows.

Первоначально, отсутствие готовых решений в этой области восполняли такие сторонние производители, как Patchlink (Update Patch Management, GravityStorm (Service Pack Manager 2000), St. Bernard Software (UpdateEXPERT и Shavlik Technologies (HFNetChkPro. Microsoft заключила контракт с Shavlik Technologies на разработку утилиты HFNetChk, работающей из командной строки, функционально ограниченной версии инструмента компании, обеспечивающей только функциональные возможности по составлению отчетов. И хотя утилита HFNetChk не может в полной мере состязаться с более совершенными (включающими возможности развертывания заплат), основанными на использовании графического интерфейса инструментами, она была бесплатной и позволяла провести учет заплат не только для ОС Windows NT 4.0 или более поздних версий, но также для ряда приложений Microsoft, таких как SQL Server, Exchange Server, Windows Media Player и Internet Explorer. Ее сканирующее ядро впоследствии было использовано в инструменте Microsoft Baseline Security Analyzer (MBSA, также разработанном для Microsoft компанией Shavlik Technologies (его версия 1.0 была выпущена в марте 2002 года). Как и ее предшественница, MBSA был ограничен подготовкой отчетов, но предлагал улучшенные возможности сканирования, а также работу как из командной строки, так и из графического пользовательского интерфейса.

Для поставки пользователям рентабельного решения по развертыванию заплат, которое также позволило бы им централизованный контроль над тем, какие заплаты уже установлены, в июне 2002 года Microsoft выпустила службу Software Update Services (SUS) 1.0 (в настоящее время на стадии SP1 – выход v2.0 ожидается в первом квартале 2004 года). Доступная для свободной загрузки, SUS реализует преимущества компонента Windows Update (что ограничивает его использование Windows 2000 и более поздними ОС) и использует основанные на интранет, корпоративные серверы Windows Update, с которых внутренние клиентские компьютеры получают проверенные обновления. Параметры обновления клиентов могут быть заданы с помощью групповых политик, в то время как настройки сервера конфигурируются с помощью интуитивно понятного, основанного на IE, интерфейса. Поскольку SUS не предоставляет какой-либо функциональности по составлению отчетов по инвентаризации, необходимо сочетать ее с MBSA или иным сопоставимым по возможностям инструментом.

Также Microsoft разработала комплексное решение по развертыванию заплат, как часть Feature Pack – дополнения (add-on) к Systems Management Server (SMS 2.0 (без дополнительной платы за the Feature Pack; чтобы использовать его, нужно просто приобрести и развернуть SMS 2.0). Feature Pack комбинирует инвентаризацию (его сканирующий процесс использует Microsoft Baseline Security Analyzer) и развертывание. В недавно выпущенную SMS 2003 были встроены дополнительные улучшения в области управления заплатами. Последующие статьи этой серии будут рассказывать об этих инструментах, а также о наборе подобных продуктов сторонних производителей.

Подобные улучшения в управлении заплатами упростили задачу поддержания безопасности сред Windows. Хотя выпуск ОС Longhorn с ее революционными изменениями в этой области отложен на некоторое время, последние инициативы Microsoft принесли значимые улучшения. Например, число заплат, для которых не требуется перезагружать систему, постоянно увеличивается.

Бесплатная утилита QCHAIN.EXE позволяет объединять несколько исправлений (hot fixe в единый пакет (для подробностей и разъяснений, посмотрите статью 296861 из Базы Знаний (КВ) Microsoft). Стратегия Microsoft на ограничение обновлений только отдельными заплатами отменена, что привело к выпуску Update Rollup 1 for Windows XP в октябре 2003 года. Это упрощает применение заплат, выпущенных после Windows-XP-SP1 для вновь устанавливаемых систем. Ожидается, что скоро заплаты будут доступны в формате .MSI, устраняющим необходимость создания индивидуальных пакетов в тех средах, где используется развертывание на основе групповых политик. Возможно, однажды Windows Update будет предлагаться даже в виде Web-службы, помогающей разработчикам создавать внутренние решения по развертыванию обновлений, основанные на технологии .NET.

В основном, решения по управлению заплатами используют подход, очень похожий на инвентаризацию и развертывание, хотя ясно, что детали реализации могут различаться. Инвентаризация опирается на внутреннюю БД в определении того, что рассматривается как рекомендуемый уровень заплат и предоставляет критерий для обоснования того, какая именно заплата должна устанавливаться. Продукты от Microsoft и Shavlik Technologies (на которых основаны HFNetChk, MBSA и SMS 2.0 Feature Pack, отслеживают опубликованные на Web-сайте Microsoft заплаты с помощью такого же механизма, основанного на файле, форматированном в XML, называемом mssecure.xml. Этот файл, доступный централизованно в предварительно установленных расположениях, служит в качестве шаблона, с которым сравнивается состояние обновлений на целевых системах. mssecure.xml может быть получен напрямую или в его сжатой, с цифровой подписью версии, mssecure.cab. Оба файла могут быть загружены с:

Web-сайта Microsoft по ссылкам https://www.microsoft.com/technet/security/search/mssecure.xml и http://download.microsoft.com/download/xml/security/1.0/nt5/en-us/mssecure.cab

Web-сайта Shavlik.com по ссылкам https://xml.shavlik.com/mssecure.xml и http://xml.shavlik.com/mssecure.cab

Вы можете открыть файл mssecure.xml в Internet Explorer и просмотреть его содержание. Начиная с версии 5, этот браузер имеет встроенный анализатор (parser XML. Для более старых версий, установите XML Parser v4, который можно загрузить по ссылке http://msdn.microsoft.com/library/default.asp?url=/downloads/list/xmlgeneral.asp. В качестве альтернативы вы можете использовать любой другой инструмент, содержащий анализатор XML (например, бесплатно загружаемый XML Notepad). mssecure.xml содержит довольно детализированную информацию о каждом обновлении, такую как: версию целевой операционной системы и уровень пакета обновления, соответствующую статью в Базе Знаний (КВ) Microsoft и ссылочный номер бюллетеня безопасности, затрагиваемые продукты и идентификаторы (ID) пакетов обновления, создаваемые ключи реестра, версию файла, контрольную сумма и расположение, а также требования по перезагрузке.

Кроме того, подавляющее большинство сторонних производителей поддерживает свои собственные механизмы проверки того, какие обновления должны быть установлены (через их собственные процедуры тестирования), а также распределения проверенных заплат. Они могут также применять индивидуальные алгоритмы проверки для определения того, была ли заплата успешно установлена (инструменты компаний Microsoft и Shavlik Technologies поддерживают одинаковый алгоритм).