SoftControl

Продуктовая линейка 4.4.12

Примечания к выпуску

Введение

Назначение

Продуктовая линейка 4.4.12 компании Safe'N'Sec Corporation предлагает набор программных компонентов для развёртывания системы информационной безопасности. Система предназначена для обеспечения целостности программной среды конечных точек сети и защиты данных от несанкционированного доступа со стороны обслуживающего персонала или злоумышленников.

В продуктовую линейку входят следующие модули:

- SoftControl Service Center («Сервисный Центр») в составе:
  - SoftControl Server – серверный компонент;
  - SoftControl Admin Console – консоль управления;
- SoftControl ATM Client / Endpoint Client / SClient / SysWatch – клиентские компоненты проактивной защиты устройств самообслуживания, рабочих станций корпоративной сети, серверов и персональных компьютеров соответственно;
- SoftControl DLP Client – клиентский компонент мониторинга и сбора данных об активности пользователя.

Настоящий документ представляет основные изменения и новые возможности, вошедшие в версию 4.4.12.

SoftControl Service Center

Улучшения и новые возможности:

1. Создание в SoftControl Admin Console и передача на клиентские хосты с установленным SoftControl SysWatch правил контроля активности для отдельных приложений. По умолчанию данная возможность отключена; включается выставлением флажка **Использовать частные настройки для модулей** в окне **Редактирование настроек клиентов** в SoftControl Admin Console.
2. Увеличена надежность хранения паролей от базы данных SoftControl Service Center и клиентских компонентов SoftControl SysWatch.
3. Оптимизирован алгоритм подписи конфигурационного файла для обновления компонентов.
4. Обновлены версии сторонних компонентов (OpenSsl и др.), используемых SoftControl, с целью закрытия известных уязвимостей в этих компонентах.
5. Изменены названия некоторых опций и кнопок.

Устранённые дефекты:

1. Дублирование в базе данных событий при наличии связанных с ними нотификаций.
2. Ошибка обновления SoftControl Admin Console, установленной отдельно от SoftControl Server.
3. Ошибка в работе правил, созданных для отдельных приложений в SoftControl Admin Console, после применения настроек на клиентских хостах с SoftControl SysWatch.
4. Исправлена логика принятия решения в случае конфликта настроек управления инцидентами и правил контроля активности для отдельных приложений. Теперь приоритет имеют настройки управления инцидентами.

Решение:

Устранено в версии 4.4.12.

SoftControl Admin Console

Улучшения и новые возможности:

1. Для файлов на вкладке **Данные профиля для...** поддержаны флаги, указывающие, был ли файл добавлен в профиль инсталлятором или в процессе сбора профиля.

2. Поддержана сортировка клиентских хостов по имени при создании задачи.
3. Журналы событий сделаны более подробными и понятными, в том числе, улучшен формат выдаваемой информации в поле **Действие** на вкладке **Лог**.
4. Логика ведения системных отчётов сделана более понятной и однозначной. Группы событий теперь называются "Угрозы" и "Службы и неподозрительные приложения". В первом случае логируются случаи нарушения политики контроля и запуск подозрительных процессов, во втором – события служб и запуск неподозрительных процессов.

Устранённые дефекты:

1. Ошибка при запросе расширенных данных профиля (вкладка **Данные профиля для...**), если на клиентском хосте ещё не был собран профиль. Теперь присылается пустой файл.
2. Ошибка, при которой на вкладке **Данные профиля для...** отображались не все файлы из профиля.
3. Ошибка при работе с SoftControl Admin Console под разными пользователями.
4. Ошибка в интерфейсе SoftControl Admin Console при создании правил политики контроля для модулей.

Решение:

Устранено в версии 4.4.12.

SoftControl Server

Устранённые дефекты:

Исправлена ошибка обновления общего клиентского сертификата.

Решение:

Устранено в версии 4.4.12.

SoftControl SysWatch

Улучшения и новые возможности:

1. Журналы событий сделаны более подробными и понятными. В частности, теперь в отчёте указывается, есть ли приложение в профиле, является ли оно отслеживаемым, имеет ли инсталлятор действительную ЭЦП, включен ли глобальный режим обновления ПО, и др.
2. Улучшен формат отчёта о сканировании.
3. Логика ведения системных отчётов сделана более понятной и однозначной. Группы событий теперь называются "Угрозы" и "Службы и неподозрительные приложения". В первом случае логируются случаи нарушения политики контроля и запуск подозрительных процессов, во втором – события служб и запуск неподозрительных процессов.
4. Удалена возможность назначать учётную запись "Ограниченный пользователь" для доверенных приложений.
5. Увеличена надежность хранения паролей от клиентских компонентов SoftControl SysWatch.
6. Устранена уязвимость, связанная с работой инсталлятора msiexec. Запрещено выполнение системного инсталлятора msiexec из папки, отличной от %SYSTEM32%.
7. Устранена уязвимость в алгоритме запрета загрузки dll (CVE-2018-5718), которая могла привести к BSOD или модификации памяти ядра ОС путём загрузки специально подготовленной dll. Исправлено для версий, начиная с 4.4.1; проявляется в версиях до 4.4.1.
8. Улучшено сообщение, выдаваемое при блокировках процессов по причине их завершения.
9. Обновлена терминология, используемая в программе. В частности, термин "режим установки" изменён на "режим обновления ПО", "неизвестная программа установки" – на "неподписанная программа установки", "неизвестное приложение" – на "приложение не в профиле", и др. Изменены названия некоторых опций и кнопок в GUI.
10. Обновлена документация, в том числе описание принципов работы программы.

Устранённые дефекты:

1. Некорректная обработка поврежденного файла, содержащего список объектов в профиле.
2. Ряд ошибок в синхронизации потоков и в работе с операционной системой, в результате чего работа SoftControl SysWatch стала стабильнее (раньше в редких случаях были

зависания ОС и падения в синий экран, а также ложные блокировки SoftControl SysWatch).

3. Некорректная обработка инцидентов нарушения политики контроля (действие запрещалось при выставленном разрешении на него в настройках).
4. Ошибка, при которой невозможно было удалить файлы из профиля.
5. Ошибка при сохранении файла с профилем системы.
6. Отключена возможность добавить файл в профиль или удалить файл из профиля, если выключена опция **Использовать профиль системы** или отключен контроль приложений.
7. Статус приложения, отображаемый в столбце **Профиль** в окне **Отслеживаемые приложения**, не соответствовал его реальному статусу.

Решение:

Устранено в версии 4.4.12.

SoftControl DLP Client

Устранённые дефекты:

Ряд ошибок в синхронизации потоков и в работе с операционной системой, в результате чего работа SoftControl DLP Client стала стабильнее (раньше в редких случаях были зависания ОС и падения в синий экран).

Решение:

Устранено в версии 4.4.12.

Техническая поддержка

При возникновении вопросов по установке, настройке и работе продуктов Safe'N'Sec Corporation вы можете обращаться в техническую поддержку по электронной почте support@safensoft.com.