ФОРСАЙТ

Форсайт. Мобильная платформа

Версия 20.08 Новые возможности

Версия от 31.08.2020

О продукте «Форсайт. Мобильная платформа»

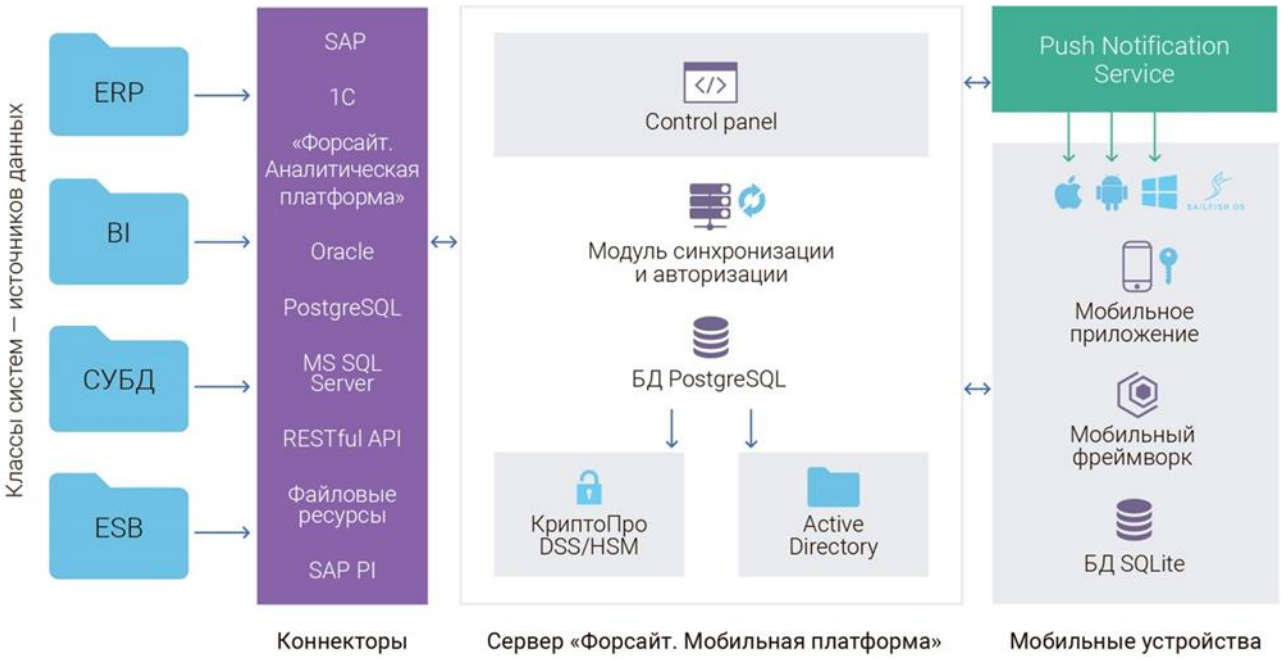
«Форсайт. Мобильная платформа» (далее – ФМП) – современный продукт на рынке Mobile Application Development Platform (MADP). Платформа обладает комплексным решением по информационной безопасности и универсальным инструментарием для быстрой и эффективной разработки защищенных мобильных приложений на основе популярных мобильных операционных систем - iOS, Android, Windows, Sailfish.

Продукт позволяет создавать надежные сервисы для обмена данными между источниками и приложениями – как нативными, так и кроссплатформенными веб-приложениями.

Возможности «Форсайт. Мобильной платформы»:

- Поддержка мобильных операционных систем - iOS, Android, Windows, Sailfish.
- Подключение различных источников данных: SAP, 1С (SOAP/XML), PostgreSQL (включая версию Pro), Oracle Database, Microsoft SQL Server, JSON SOAP/XML веб-сервисы, Microsoft Exchange, проектирование HTTP-запросов, продукт «Форсайт. Аналитическая платформа», файловые ресурсы.
- Передача справочных и оперативных данных. Снижение нагрузки на бизнес-системы за счет кэширования данных в платформе.
- Значительное ускорение передачи данных за счет определения только измененной информации (расчет дельты), фильтрации и разделения блоков данных по параметрам.
- Встроенные источники «Локальная БД» и «Локальное файловое хранилище».
- Доступ к данным в онлайн и офлайн-режиме.
- Обеспечение информационной безопасности:
  - единая точка аутентификации для пользователей мобильных устройств;
  - аутентификация и авторизация в корпоративных системах;
  - использование шифрования;
  - шифрование сетевого трафика между сервером и мобильным устройством;
  - разделение полномочий администраторов и команд проектов в консоли администратора;
  - журналирование поведения системы и действий пользователей.
- Разработка мобильного приложения с использованием фреймворка.
- Интеграция с MDM (Citrix XenMobile).

Архитектура продукта



Мы развиваем и улучшаем инструментарий продукта «Форсайт. Мобильная платформа» в соответствии с требованиями рынка и наших партнеров. Для версии 20.08.11 выбраны следующие направления развития.

Серверные компоненты

Авторегистрация и синхронизация в Active Directory

Новая версия позволяет настроить авторегистрацию пользователей на основании записей Active Directory. После проверки в Active Directory, пользователи могут пользоваться сервисами мобильной платформы (учётная запись в мобильной платформе создаётся автоматически).

Мы добавили возможность отключить полную синхронизацию членства в группах безопасности Active Directory в консоли администратора.

Теперь можно оперативно работать с группами LDAP: сокращено время на первоначальную синхронизацию групп, в которых тысячи пользователей.

Персональный кэш

Для пользователей Active Directory реализована поддержка автоматического разделения персонального кэша для всех источников. При обращении пользователя к ресурсам источника данных автоматически формируется персональный кэш, доступный только пользователю.
Включить функцию можно в консоли администратора – выбрать для источника данных «использование учетных данных LDAP».

Формат хранения данных пользователя

Формат хранения данных пользователя Active Directory теперь заменен на более распространенный – domain\username. В этом формате пользователям будут доступны push-уведомления.
Сервер «Форсайт. Мобильной платформа» продолжит поддерживать прежний формат username@domain: будет автоматически конвертировать его в актуальный и сравнивать для идентификации.

GET-параметры для JSON-коннектора

Мы реализовали возможность отправки GET-параметров с мобильного устройства для поддержки механизма интеграции с JSON-источниками и внедрили механизм выделения кэша по уникальному набору GET-параметров.

При настройке ресурса для источника JSON на консоли администратора можно добавить GET-параметры, которые требуется указать на самом сервере или передать мобильному приложению. Прежние GET-параметры будут автоматически перенесены в новый механизм при обновлении сервера.

Новый механизм определения уникальности и разделения кэша не обрабатывает перечисление значений с одинаковым названием параметра (пример: param1=value1:param1=value2), поэтому рекомендуем их отправлять в одном параметре через запятую.

Данные кэша при запросе несуществующих версий

Мы оптимизировали алгоритм для запросов на получение кэша с несуществующей (устаревшей) версии на сервере. Теперь при таком запросе система уведомляет об ошибке. Фреймворки автоматически удалят неактуальную информацию и загрузят кэш актуализированными данными.

Список исправленных ошибок

- При добавлении или удалении прав на системные логи и прав доступа ко всем средам отсутствует описание.
- При импортировании группы пользователей из LDAP в поиске содержатся системные группы.
- При импортировании 2 групп из LDAP с одинаковым пользователем в каждой, пользователю присваивается только 1 группа.

Список улучшений функционала

- Добавлена обработка алгоритма для перезагрузки кэша при невозможности рассчитать дельту на севере (устаревшая версия кэша).
- Исправлены минорные замечания.
- Расширено логирование для работы с сетью и с базой данных на мобильном устройстве.

Анализ ПО в поставке «Форсайт. Мобильной платформы» (CVE) на известные ошибки безопасности

Для поставки сервера «Форсайт. Мобильной платформы» (версия 20.08.01) произведен анализ образов контейнеров на наличие уязвимостей в соответствии с CVE. Анализ проводится ПО Clair: https://github.com/quay/clair.
В версии 20.08.01 отсутствуют замечания уровня Critical.
В версии 20.08.01 присутствуют образы контейнеров внешних компонентов Filebeat, Elastic и Kibana, которые содержат уязвимости уровня High.
В результате проверки определили, что в текущей архитектуре компоненты находятся в виртуальной изолированной сети docker и недоступны для подключения из любой другой сети. Данные уязвимости не применимы.

Известные ошибки безопасности ПО в поставке ФМП

Elastic

RHSA-2020:0227: [High]
Found in: sqlite [3.7.17-8.el7]
Fixed By: 0:3.7.17-8.el7_7.1
SQLite is a C library that implements an SQL database engine. A large subset of SQL92 is supported. A complete database is stored in a single disk file. The API is designed for convenience and ease of use. Applications that link against SQLite can enjoy the power and flexibility of an SQL database without the administrative hassles of supporting a separate database server. Security Fix(es): * sqlite: fts3: improve shadow table corruption detection (CVE-2019-13734) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

https://access.redhat.com/errata/RHSA-2020:0227

Kibana

RHSA-2020:0227: [High]
Found in: sqlite [3.7.17-8.el7]
Fixed By: 0:3.7.17-8.el7_7.1
SQLite is a C library that implements an SQL database engine. A large subset of SQL92 is supported. A complete database is stored in a single disk file. The API is designed for convenience and ease of use. Applications that link against SQLite can enjoy the power and flexibility of an SQL database without the administrative hassles of supporting a separate database server. Security Fix(es): * sqlite: fts3: improve shadow table corruption detection (CVE-2019-13734) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.
https://access.redhat.com/errata/RHSA-2020:0227

RHSA-2019:4190: [High]
Found in: nss-util [3.44.0-3.el7]
Fixed By: 0:3.44.0-4.el7_7
Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications. The nss-softokn package provides the Network Security Services Softoken Cryptographic Module. The nss-util packages provide utilities for use with the Network Security Services (NSS) libraries. Security Fix(es): * nss: Out-of-bounds write when passing an output buffer smaller than the block size to NSC_EncryptUpdate (CVE-2019-11745) * nss: Empty or malformed p256-ECDH public keys may trigger a segmentation fault (CVE-2019-11729) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.
https://access.redhat.com/errata/RHSA-2019:4190

RHSA-2019:4190: [High]
Found in: nss-tools [3.44.0-4.el7]
Fixed By: 0:3.44.0-7.el7_7
Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications. The nss-softokn package provides the Network Security Services Softoken Cryptographic Module. The nss-util packages provide utilities for use with the Network Security Services (NSS) libraries. Security Fix(es): * nss: Out-of-bounds write when passing an output buffer smaller than the block size to NSC_EncryptUpdate (CVE-2019-11745) * nss: Empty or malformed p256-ECDH public keys may trigger a segmentation fault (CVE-2019-11729) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.
https://access.redhat.com/errata/RHSA-2019:4190

RHSA-2019:4190: [High]
Found in: nss-sysinit [3.44.0-4.el7]
Fixed By: 0:3.44.0-7.el7_7
Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications. The nss-softokn package provides the Network Security Services Softoken Cryptographic Module. The nss-util packages provide utilities for use with the Network Security Services (NSS) libraries. Security Fix(es): * nss: Out-of-bounds write when passing an output buffer smaller than the block size to NSC_EncryptUpdate (CVE-2019-11745) * nss: Empty or malformed p256-ECDH public keys may trigger a segmentation fault (CVE-2019-11729) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.
https://access.redhat.com/errata/RHSA-2019:4190

RHSA-2019:4190: [High]
Found in: nss [3.44.0-4.el7]
Fixed By: 0:3.44.0-7.el7_7
Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications. The nss-softokn package provides the Network Security Services Softoken Cryptographic Module. The nss-util packages provide utilities for use with the Network Security Services (NSS) libraries. Security Fix(es): * nss: Out-of-bounds write when passing an output buffer smaller than

the block size to NSC_EncryptUpdate (CVE-2019-11745) * nss: Empty or malformed p256-ECDH public keys may trigger a segmentation fault (CVE-2019-11729) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.
https://access.redhat.com/errata/RHSA-2019:4190

RHSA-2020:0227: [High]
Found in: sqlite [3.7.17-8.el7]
Fixed By: 0:3.7.17-8.el7_7.1
SQLite is a C library that implements an SQL database engine. A large subset of SQL92 is supported. A complete database is stored in a single disk file. The API is designed for convenience and ease of use. Applications that link against SQLite can enjoy the power and flexibility of an SQL database without the administrative hassles of supporting a separate database server. Security Fix(es): * sqlite: fts3: improve shadow table corruption detection (CVE-2019-13734) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.
https://access.redhat.com/errata/RHSA-2020:0227

RHSA-2019:4190: [High]
Found in: nss-softokn-freebl [3.44.0-5.el7]
Fixed By: 0:3.44.0-8.el7_7
Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications. The nss-softokn package provides the Network Security Services Softoken Cryptographic Module. The nss-util packages provide utilities for use with the Network Security Services (NSS) libraries. Security Fix(es): * nss: Out-of-bounds write when passing an output buffer smaller than the block size to NSC_EncryptUpdate (CVE-2019-11745) * nss: Empty or malformed p256-ECDH public keys may trigger a segmentation fault (CVE-2019-11729) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.
https://access.redhat.com/errata/RHSA-2019:4190

RHSA-2019:4190: [High]
Found in: nss-softokn [3.44.0-5.el7]
Fixed By: 0:3.44.0-8.el7_7
Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications. The nss-softokn package provides the Network Security Services Softoken Cryptographic Module. The nss-util packages provide utilities for use with the Network Security Services (NSS) libraries. Security Fix(es): * nss: Out-of-bounds write when passing an output buffer smaller than the block size to NSC_EncryptUpdate (CVE-2019-11745) * nss: Empty or malformed p256-ECDH public keys may trigger a segmentation fault (CVE-2019-11729) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.
https://access.redhat.com/errata/RHSA-2019:4190
