ФОРСАЙТ

Форсайт. Мобильная платформа

Версия 20.10.01
Новые возможности

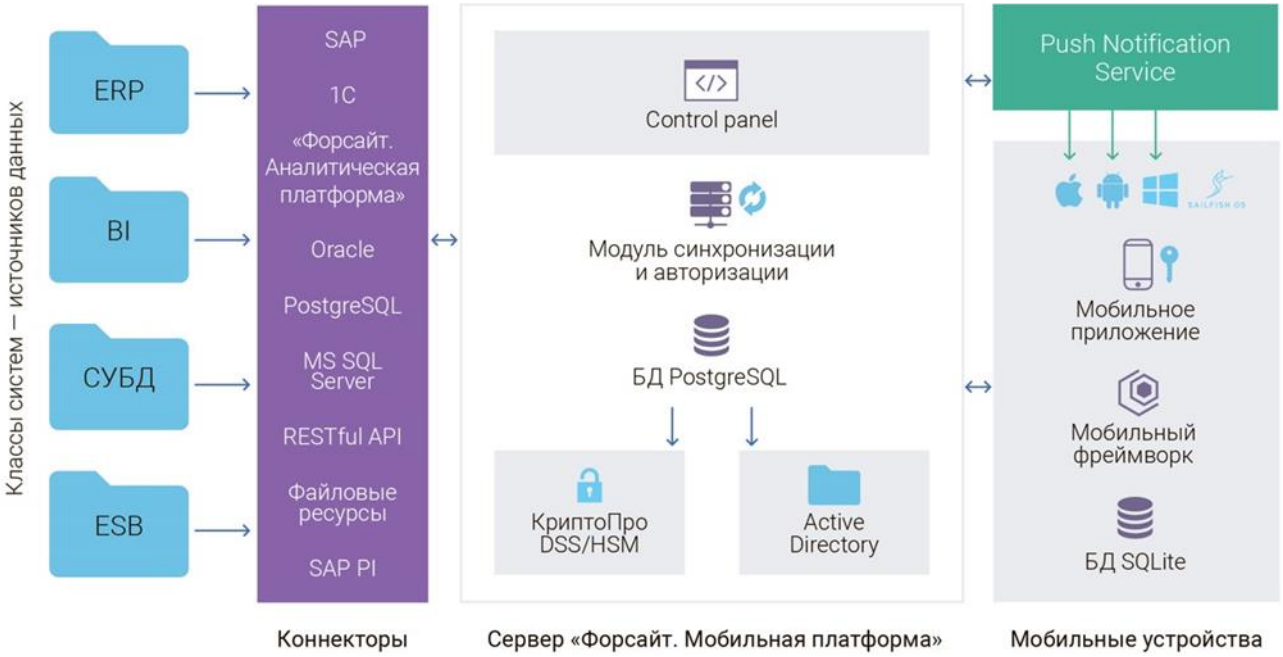
О ПРОДУКТЕ «ФОРСАЙТ. МОБИЛЬНАЯ ПЛАТФОРМА»

«Форсайт. Мобильная платформа» – 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.

Ключевые возможности:

- 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 и 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 изменённой 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).


Классы систем – источников данных
ERP
BI
СУБД
ESB
SAP
1С
«Форсайт. Аналитическая платформа»
Oracle
PostgreSQL
MS SQL Server
RESTful API
Файловые ресурсы
SAP PI
Control panel
Модуль синхронизации и авторизации
БД PostgreSQL
КриптоПро DSS/HSM
Active Directory
Push Notification Service
Мобильное приложение
Мобильный фреймворк
БД SQLite
Коннекторы
Сервер «Форсайт. Мобильная платформа»
Мобильные устройства

СЕРВЕРНЫЕ КОМПОНЕНТЫ «ФОРСАЙТ. МОБИЛЬНОЙ ПЛАТФОРМЫ»

Аутентификация Kerberos для источников данных JSON, SOAP, 1C и web-ресурсов

Для сервера «Форсайт. Мобильной платформы» теперь можно настроить централизованное подключение к серверу аутентификации Kerberos. Kerberos-аутентификация доступна для источников данных JSON, SOAP, 1C и web-ресурсов и позволяет получить TGT, TGS-тикет для дальнейшей авторизации.

Поддержка динамических URL для web-ресурсов

Для web-ресурсов возможно использовать динамические URL при отправке API-запроса на сервер «Форсайт. Мобильной платформы».

В настройках web-ресурса возможно задать параметр «Путь по умолчанию». Если при обращении к ресурсу в API-запросе не указан путь в источнике данных, запрос будет отправлен по пути, указанному по умолчанию. Если в API-запросе указан путь к ресурсу в источнике данных, запрос будет отправлен по данному пути.

Проверка целостности данных при отправке на мобильное устройство

Для всех источников данных, запрашиваемых через API-методы RPC-ресурсов, добавлена проверка целостности данных. При получении сервером «Форсайт. Мобильной платформы» API-запроса производится расчет хэш-суммы по id каждой записи, хэш-сумма отправляется в ответе на запрос на мобильное устройство. Мобильное устройство рассчитывает хеш по данным, и если они не совпадают с хэшем с сервера, то данные для этого ресурса автоматически обновляются.

Смена и сброс пароля для учетных записей администраторов

Администраторы сервера могут сбросить пароль для учетной записи своих коллег или поменять свой пароль в консоли администратора. Для каждого действия выполняется отдельная запись в журнале событий.

API-методы для обновления кеша

Теперь любой кеш в мобильной платформе можно обновить не только по расписанию и запросу пользователя, но и с помощью отдельного API-интерфейса. Источники данных оперативно сообщат серверу «Форсайт. Мобильной платформы», когда ему нужно обновить закешированные данные.

Дополнительные изменения в платформе

- Параметры «Время жизни сессии при неактивности администратора».
- API-методы для обновления конкретного кеша и получения статуса его обновления.
- Добавлена возможность отправки push-уведомлений на iOS-устройства через Firebase Cloud Messaging.
- Для push-уведомлений добавлен параметр «Время хранения push-уведомлений».
- Для ресурса источника данных JSON добавлена возможность указания нескольких параметров.
- В системные логи добавлено событие «Выход из системы».
- Заменен wsgi-сервер.
- Контейнер celery разделен на контейнеры beat и worker.
- В кластерной конфигурации возможно масштабировать nod’ы cache_standby за счет разделения READ и WRITE операций.
- Настройки SSH-ключа вынесены в .env файл. Исключена необходимость обновления Relay-сервера при обновлении сервера «Форсайт. Мобильной платформы».
- В конфигурации Standalone добавлен параметр автоматического перезапуска контейнеров при перезагрузке физического сервера.
- Сокращен общий размер архива с Docker образами за счет удаления неактуальной информации.

МОБИЛЬНЫЕ КОМПОНЕНТЫ «ФОРСАЙТ. МОБИЛЬНОЙ ПЛАТФОРМЫ»

1. Проверка целостности данных на мобильном устройстве

На мобильном устройстве производится расчет хэш-суммы по id записей ресурса. Проводится сравнение хэш-суммы, рассчитанной на мобильном устройстве, и хэш-суммы, полученной от сервера «Форсайт. Мобильной платформы». Если хэш-суммы совпадают, целостность данных считается ненарушенной. Если они не совпадают, то данные повторно запрашиваются с сервера «Форсайт. Мобильной платформы». Если при повторном сравнении хэш-суммы не совпадают, данные на мобильном устройстве не перезаписываются и возвращается ошибка.

2. Расширено логирование для фреймворков

Выделено 4 типа логов:

1.Verbose – самая детальная информация.

2.Debug – отладочная информация.

3.Warning – предупреждения.

Расширена функциональность работы с логами.

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

Для поставки сервера «Форсайт. Мобильной платформы» версии 20.10.01 произведен анализ образов контейнеров на наличие уязвимостей в соответствии с CVE. Анализ проводится ПО Clair: https://github.com/quay/clair

В данной версии нет замечаний уровня Critical.

В данной версии содержатся 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, входящего в поставку «Форсайт. Мобильной платформы»

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

Filebeat

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
