

Меры обеспечения безопасности платформы SMBC MiVoice Office 400

Информация о редакции документа

Версия	Дата выпуска	Действительна для
1,1	11.21.2023	Обновленная контактная информация
1,0	03.12.2018	Платформа SMBC Mitel Office 400

Информация, содержащаяся в настоящем документе, конфиденциальна, является собственностью компании Mitel® и предназначена исключительно для сотрудников Mitel и официальных органов контроля за торговой деятельностью, которым требуется данная информация. Если вы не являетесь сотрудником Mitel или официальным органом контроля за торговой деятельностью, вы не являетесь предполагаемым получателем данной информации. Пожалуйста, удалите или верните любые сопутствующие материалы. Mitel будет обеспечивать соблюдение своего права на защиту конфиденциальной и служебной информации, и несоблюдение вышеуказанных условий может привести к принятию судебных мер в отношении вас или вашей компании.

Содержание

Информация о редакции документа	2
1 Цель	4
2 Область применения	4
3 Информация о версии	5
4 Сведения об операционной системе	5
5 Меры обеспечения безопасности	6
5.1 Меры обеспечения безопасности сигнализации	6
5.1.1 Используемое шифрование сигнализации	6
5.1.2 Зависимость от поставщиков программного обеспечения	6
5.2 Меры обеспечения безопасности передаваемых данных	6
5.2.1 Используемое шифрование мультимедиа	6
5.2.2 Зависимость от поставщиков программного обеспечения	6
5.3 Меры обеспечения безопасности управления службами	6
5.3.1 Используемое шифрование служб	6
5.3.2 Зависимость от поставщиков программного обеспечения	7
5.4 Меры обеспечения безопасности аутентификации	7
5.4.1 Используемый механизм	7
5.4.2 Зависимость от поставщиков программного обеспечения	7
5.5 Меры обеспечения безопасности - другое	7
5.5.1 Используемый механизм	7
5.5.2 Зависимость от поставщиков программного обеспечения	7
6 Идентификация продукта Mitel	8
7 Рынки/Формы распространения	8
8 Контактное лицо	8

1 ЦЕЛЬ

Настоящий документ содержит информацию о мерах обеспечения безопасности системы связи MiVoice Office 400, где основное внимание уделено платформе SMBC. В нем перечислены модули безопасности и используемые механизмы, а также различия программных модулей безопасности.

2 ОБЛАСТЬ ПРИМЕНЕНИЯ

MiVoice Office 400 версии R6.0 (09.2018). В данном документе говорится только о контроллере SMB (SMBC) системы связи MiVoice Office 400.

Обзор MiVoice Office 400 и относящихся к нему механизмов обеспечения безопасности в целом приведены в документе "MiVoice Office 400 Product Description" (depl-1623). Этот документ является дополнением к вышеупомянутому документу в отношении зависимости программных модулей безопасности от оригинальных производителей.

3 ИНФОРМАЦИЯ ОБ ИЗДАНИИ

Настоящий документ содержит информацию о платформе SMBC и ее встроенном программном обеспечении по состоянию на сентябрь 2018.

В Mivoice Office 400 реализованы следующие параметры безопасности:

- Безопасная сигнализация управления вызовами с помощью TLS, например, SIP
- Безопасная передача мультимедийных данных с помощью SRTP
- Безопасное управление службами, такими как HTTPS и SMTP, с помощью TLS
- Безопасное управление службами с помощью SSH для удаленного доступа

Для использования перечисленных выше методов обеспечения безопасности для "сигнализации для управления вызовами" и для "передачи мультимедийных данных" требуется специальная лицензия безопасности. Для всех остальных защищенных сервисов это доступно по умолчанию.

4 СВЕДЕНИЯ ОБ ОПЕРАЦИОННОЙ СИСТЕМЕ

Операционная система, используемая для SMBC, основана на Linux. Под Linux понимается так называемый встроенный дистрибутив Linux, который использует стандартное ядро Linux версии 4.x. Для обеспечения безопасности в системе Linux были настроены соответствующие компоненты.

5 МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Меры безопасности для SMBC могут быть разделены на службы, относящиеся к сигнализации служб телефонии, обработку голосовых данных и глобальные службы на основе IP в качестве базового уровня.

5.1 МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СИГНАЛИЗАЦИИ

Меры обеспечения безопасности сигнализации для вызовов VoIP используют протокол защиты транспортного уровня (TLS) на SMBC.

5.1.1 ИСПОЛЬЗУЕМОЕ ШИФРОВАНИЕ СИГНАЛИЗАЦИИ

Для шифрования сигнализации SMBC использует протокол TLS версии 1.2 (TLSv1.2). Для протоколов диалога и записей в TLS используется алгоритм генерации подписей SHA512 с RSA. Размер ключа сервера составляет 1024 бита RSA, и создание отпечатка пальца осуществляется с помощью SHA1/SHA256. Используемые шифры: AES256-GCM-SHA384, AES256-SHA256, AES256-SHA, CAMELLIA256-SHA, AES128-GCM-SHA256, AES128-SHA256, AES128-SHA, SEED-SHA и CAMELLIA128-SHA.

Для использования сертификата сервера SMBC использует самозаверяющие сертификаты, которые генерируются внутренним УЦ (Удостоверяющий центр).

5.1.2 ЗАВИСИМОСТЬ ОТ ПОСТАВЩИКОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Функциональность TLS, используемая в SMBC, это открытое программное обеспечение, которое называется "OpenSSL" и распространяется фондом "OpenSSL Software Foundation". Библиотека OpenSSL статически связана с операционной системой (ОС) SMBC. Все используемые функции обмена данными TLS - из собственной библиотеки OpenSSL. В версии 6.0 GA в SMBC используется OpenSSL версии 1.0.2 j.

5.2 МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРЕДАВАЕМЫХ ДАННЫХ

Меры по обеспечению безопасности передаваемых данных для вызовов VoIP реализованы в цифровом сигнальном процессоре (DSP), который расположен на материнской плате SMBC. В дополнение к данному оборудованию к материнской плате SMBC могут быть подключены модули или карты с чипами DSP. Используются DSP серии C55x производства компании Texas Instruments. Обратите внимание, что защищенные каналы VoIP должны быть настроены в конфигурации. Кроме того, для всех безопасных медиа-потоков обязательна активация безопасной сигнализации с помощью TLS.

5.2.1 ИСПОЛЬЗУЕМОЕ ШИФРОВАНИЕ МУЛЬТИМЕДИА

Функциональность SRTP использует расширенный стандарт шифрования (AES) для шифрования 128-битным мастер-ключом и аутентификационный жетон объемом 32 или 80 бит.

5.2.2 ЗАВИСИМОСТЬ ОТ ПОСТАВЩИКОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

DSP использует функциональность протокола SRTP, предоставленную компанией Snapfield Ltd. Исходный код, содержащий функции шифрования, включен в процесс компиляции версии программного обеспечения DSP.

5.3 МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УПРАВЛЕНИЯ СЛУЖБАМИ

Для доступа к SMBC меры обеспечения безопасности служб должны использовать либо упомянутый выше протокол защиты транспортного уровня (TLS), либо протокол "безопасной оболочки" (SSH). Службы, использующие TLS в качестве уровня безопасности, это универсальные службы, такие как почта или веб-конфигурация SMBC. Информация в отношении протокола TLS аналогична указанной выше. В подразделах ниже приведены подробные сведения о службе SSH.

Функциональность SSH, используемая в SMBC, это открытое программное обеспечение безопасной оболочки, которое является открытым исходным кодом и называется "OpenSSH". Обратите внимание, что поддержка/доступ к безопасной оболочке должны быть активированы в настройках SMBC, прежде чем ее можно будет использовать.

5.3.1 ИСПОЛЬЗУЕМОЕ ШИФРОВАНИЕ СЛУЖБ

Для шифрования служб SMBC использует SSH версии 7.3 (OpenSSH 7.3). Для алгоритмов обмена ключами используется протокол curve25519-sha256 и варианты алгоритмов ecdh-sha2-nistp и diffie-hellman-group14/16/18. Используются следующие алгоритмы ключа хоста: ssh-rsa, rsa-sha2-256, rsa-sha2-512, ssh-ed25519. Используемые шифры: chacha20-poly1305, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm и aes256-gcm. Используются следующие коды проверки подлинности сообщения: umac-64-etm, umac-128-etm, hmac-sha2-256-etm, hmac-sha2-512-etm, hmac-sha1-etm.

5.3.2 ЗАВИСИМОСТЬ ОТ ПОСТАВЩИКОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Функциональность SSH, используемая в SMBC, это открытое программное обеспечение, которое называется "OpenSSH". Библиотека OpenSSH статически связана с операционной системой (ОС) SMBC. Все используемые функции службы OpenSSH - из собственной библиотеки OpenSSH. В версии 6.0 GA в SMBC используется OpenSSH версии 7.3.

5.4 МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АУТЕНТИФИКАЦИИ

Меры обеспечения безопасности аутентификации зависят от службы, к которой идет обращение. Службы (или протоколы), предоставляемые SMBC и поддерживающие проверку подлинности, в большинстве случаев включают саму процедуру аутентификации. Службами, которые включают такую аутентификацию, являются, например, регистрация SIP или доступ к веб-серверу SMBC через HTTP(S).

5.4.1 ИСПОЛЬЗУЕМЫЙ МЕХАНИЗМ

Механизмом аутентификации, используемым упомянутыми выше протоколами (SIP/HTTP), является метод "дайджест-аутентификации". Для этого используется алгоритм вычисления хеш-функции MD5.

Кроме того, веб-сервер использует алгоритм RSA с 1024-битным ключом для процедуры входа в систему для доступа к веб-приложениям.

5.4.2 ЗАВИСИМОСТЬ ОТ ПОСТАВЩИКОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Функции механизмов аутентификации являются частью OpenSSL, смотрите подробную информацию выше.

5.5 МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ РАЗНОЕ

SMBC содержит некоторые данные, которые не связаны ни с сигнализацией, ни с обработкой медиаресурсов. Более того, к этим данным не имеют доступа службы управления, упомянутые выше. Но данные могут быть предоставлены клиенту, например, в виде файла. Такие данные также защищены благодаря тому, что резервная копия данных, создаваемая SMBC, находится в контейнере (zip-файл), содержащем зашифрованную базу данных конфигурации системы.

5.5.1 ИСПОЛЬЗУЕМЫЙ МЕХАНИЗМ

Для шифрования содержимого базы данных используется алгоритм AES_CBC_256.

5.5.2 ЗАВИСИМОСТЬ ОТ ПОСТАВЩИКОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Функции алгоритмов шифрования являются частью OpenSSL, подробную информацию смотрите выше.

6 ИДЕНТИФИКАЦИЯ ПРОДУКТА MITEL

	Примечание	Номер продукта Mitel	Дата выпуска
Контроллер SMB	Базовый контроллер SMB системы, включая ЦП, ОС и встроенный IP медиа-шлюз;	50006942	3 квартал 2018

7 РЫНКИ/ФОРМЫ РАСПРОСТРАНЕНИЯ

Система связи MiVoice Office 400 предназначена для предприятий, работающих на международном рынке. Система связи MiVoice Office 400 реализуется через косвенные каналы сбыта.

8 КОНТАКТНОЕ

Название отдела: Митель Юридический отдел

Электронная почта: legal@mitel.com

Информация, содержащаяся в настоящем документе, конфиденциальна, является собственностью компании Mitel® и предназначена исключительно для сотрудников Mitel и официальных органов контроля за торговой деятельностью, которым требуется данная информация. Если вы не являетесь сотрудником Mitel или официальным органом контроля за торговой деятельностью, вы не являетесь предполагаемым получателем данной информации. Пожалуйста, удалите или верните любые сопутствующие материалы. Mitel будет обеспечивать соблюдение своего права на защиту конфиденциальной и служебной информации, и несоблюдение вышеуказанных условий может привести к принятию судебных мер в отношении вас или вашей компании.