Содержание

Введение

Сторонний разработчик (не Cisco) выпустил программу для дешифрования паролей пользователей (и других паролей) в файлах конфигурации Cisco. **Программа не будет расшифровывать пароли, установленные с разрешением команды secret.** Непредвиденная проблема, которую данная программа вызвала у пользователей Cisco, вызвала подозрения, что многие пользователи полагаются на шифрование пароля Cisco как на средство большей безопасности, чем это было предусмотрено. В этом документе поясняется модель безопасности, на которой строится технология шифрования паролей Cisco, и особенности этого шифрования, ограничивающие безопасность.

Примечание: Cisco рекомендует, чтобы все устройства Cisco IOS внедрили модель безопасности аутентификации, авторизации и учета (AAA). В модели AAA может использоваться локальная база данных, RADIUS и TACACS+.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Пароли пользователя

Пароли пользователя и большая часть других паролей (не enable secrets) в файлах конфигурации Cisco IOS шифруются с помощью схемы, которая не отвечает всем требованиям современных криптографических стандартов.

Несмотря на то, что Cisco не распределяет программу расшифровки, по крайней мере две других программы расшифровки для паролей Cisco IOS доступны общественности в Интернете; первый релиз общего пользования такой программы, о которой Cisco знает, был в начале 1995 года. Мы ожидали бы, что любой криптограф - непрофессионал будет в состоянии создать новую программу с небольшим усилием.

Схема, используемая Cisco IOS для пользовательских паролей, не предназначена для сопротивления намеренной, хорошо спланированной атаке. Схема шифрования была создана для предотвращения кражи паролей с помощью отслеживания или прослушивания. Это никогда не предназначалось для защиты против кого-то проводящего взламывающее пароль усилие на файле конфигурации.

Из-за слабого алгоритма шифрования это всегда была позиция Cisco, что клиенты должны рассматривать любой файл конфигурации, содержащий пароли как уязвимые данные, тот же способ, которым они рассматривали бы незашифрованный список паролей.

"enable secret" и "enable password"

Команда enable password больше не должна использоваться. **Используйте разблокированную шифрованную команду для более высокой безопасности**. Единственный экземпляр, в котором могла бы быть протестирована **команда enable password**, - когда устройство работает в режиме загрузки, который не поддерживает **команду enable secret**.

Команда enable secret хешируется при помощи алгоритма MD5. Насколько известно в Cisco, невозможно восстановить включенный секретный пароль по содержимому файла конфигурации (кроме известного способа подбора пароля по словарю).

Примечание: Это применяется только к набору паролей с **enable secret**, а *не* к набору паролей с **enable password**. Действительно, сила используемого шифрования является единственным существенным различием между этими двумя командами.

Какой режим Cisco IOS Image поддерживает команду enable secret?

Воспользовавшись командой show version в обычном рабочем режиме, просмотрите загрузочный образ (полный образ Cisco IOS), чтобы выяснить, поддерживает ли этот загрузочный образ разрешающую секретную команду. Если это делает, удалите **enable password**. **Если загрузочный образ не поддерживает включение секретного пароля, необходимо учесть следующие предупреждения:**

- Установка enable password могла бы быть ненужной, если у вас есть физическая безопасность так, чтобы никто не мог повторно загрузить устройство к образу загрузки.
- Физический доступ к устройству позволяет нарушить его безопасность, не обращаясь к загрузочному образу.
- **При установке значения enable password равным значению enable secret степень**

уязвимости значения enable secret к атаке становится такой же, как у значения enable password.

- **Если параметр enable password имеет другое значение, т. к. загрузочный образ не поддерживает команду enable secret, администраторы должны будут запомнить новый пароль, который редко используется на ROM без поддержки команды enable secret.** При наличии отдельного enable password администраторы могут не помнить пароль, когда они вызывают время простоя для обновления программного обеспечения, которое является единственной причиной войти к режиму загрузки.

Другие пароли

Почти все пароли и другие строки проверки подлинности в Файлах конфигурации Cisco IOS зашифрованы с помощью слабой, обратимой схемы, используемой для паролей пользователя.

Чтобы определить, какая схема была использована для шифрования конкретного пароля, проверьте цифру, предшествующую зашифрованной строке в файле конфигурации. Если данная цифра – 7, это означает, что пароль был зашифрован с помощью слабого алгоритма. Если же это 5, значит пароль был хэширован с помощью более сильного алгоритма MD5.

Например, в команде настройки:

```
enable secret 5 $1$iUjJ$cDZ03KKGh7mHfX2RSbDqP.
```

Хэширование команды enable secret осуществляется с помощью MD5, тогда как для команды:

```
username jdoe password 7 07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D
```

Пароль зашифрован с использованием слабого обратимого алгоритма.

Файлы конфигурации

Перед передачей сведений о конфигурации в сообщении электронной почты необходимо удалить из конфигурации пароли типа 7. **Можно использовать команду show tech-support, которая по умолчанию изымает секретные данные.** Типовой **show tech-support command output** показывают ниже.

```
username jdoe password 7 07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D
```

При сохранении файлов конфигурации на сервер простейшего протокола передачи файлов (TFTP) измените полномочия на эти файлы, если они не используются, или защитите их межсетевым экраном.

Можно ли изменить алгоритм?

Cisco не имеет никаких непосредственных планов поддержать стойкий алгоритм шифрования для паролей пользователя Cisco IOS. Если Cisco должна решить представить такую функцию в будущем, та функция определенно наложит дополнительные административные накладные расходы на пользователей, которые принимают решение использовать преимущества его.

Это не, в общем случае, возможном переключать пароли пользователя на на основе MD5 алгоритм, используемый для enable secret, потому что MD5 является однонаправленным хэшированием, и пароль не может быть восстановлен с зашифрованных данных вообще. Чтобы поддержать определенные протоколы аутентификации (особенно CHAP), системный доступ потребностей к открытому тексту паролей пользователя, и поэтому должен сохранить их использующий обратимый алгоритм.

Из-за сложностей с управлением ключами переход на использование более сильного обратимого алгоритма, например DES, может оказаться непростой задачей. Несмотря на то, что было бы легко модифицировать Cisco IOS для использования DES для шифрования паролей, не было бы никакого преимущества в безопасности при этом, если бы все системы Cisco IOS использовали тот же ключ DES. Если бы разные ключи использовались разными системами, административная нагрузка была бы введена для всех сетевых администраторов Cisco IOS, и совместимость файлов конфигурации при переносе с одной системы на другую была бы нарушена. Потребность заказчиков в более серьезном обратимом шифровании пароля была небольшой.

Дополнительные сведения

- Процедуры восстановления паролей
- Руководство Cisco по усилению защиты устройств Cisco IOS
- Техническая поддержка - Cisco Systems