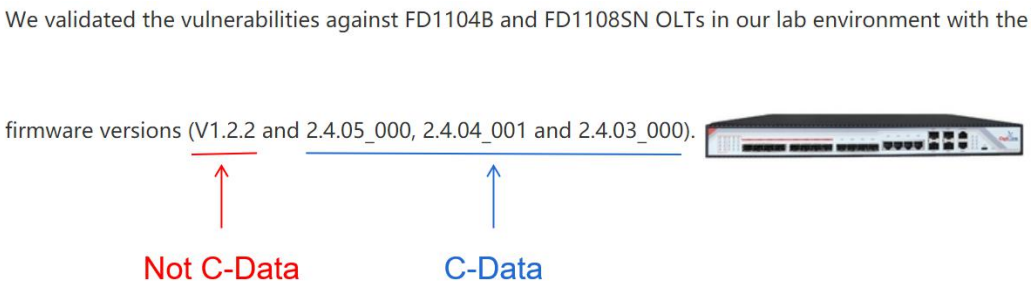
Statement on Pierre Kim Revealing Security Vulnerabilities in C-data OLT products

Мы заметили статью под названием «Многочисленные уязвимости, обнаруженные в OLT C-Data», опубликованную в Github. C-Data восхищается работой двух специалистов в технологических кругах, Пьера Кима и Александра Торреса, и благодарит их за выявление проблем с безопасностью путем подробного тестирования, а также за их активную работу по снижению рисков пользователей, использующих сетевые продукты. C-Data придерживается философии обслуживания клиентов и всегда ставит интересы клиентов на первое место, а также уделяет особое внимание проблемам безопасности продукта. Таким образом, C-Data может предоставить клиентам продукты с гарантией безопасности.

Тем временем мы обратили внимание на некоторые пресс-релизы, публикуемые средствами массовой информации, и интерпретировали технические статьи Пьера Кима и Александра Торреса. Чтобы не допустить, чтобы большинство клиентов неправильно поняли конструкцию безопасности нашего оборудования, C-Data анализирует и разъясняет указанные технические проблемы с искренним и откровенным подходом.

Исключая контрафактную продукцию



Учетная запись, упомянутая в этой статье: panger123 / suma123. Мы исследовали аккаунт и пароль. Кроме того, мы подтвердили, что учетная запись и пароль не принадлежат продуктам C-Data OLT, а используются другими компаниями и людьми при копировании C-Data OLT. Стиль CLI и большинство его команд поддельного OLT копируются из OLT C-Data. Оборудование C-Data OLT в настоящее время широко используется во всем мире, и мошеники копируют C-Data OLT для получения нелегальной прибыли.

На следующем снимке экрана мы можем полностью сравнить и проанализировать, что учетная запись panger123 / suma123 происходит от нелегально скопированного OLT.

[Replica command line style and version information]

```
$ telnet [ip]
******************************************************************
        Command Line Interface for EPON System
                Hardware Ver:  V1.2
                Software Ver:  V1.2.2
                Created Time:  Mar 12 2018 06:54:24
    Copyright (c) 2015-2020 All rights reserved.
******************************************************************
Username:panger123
Password:suma123

Entry Supperuer successfully!

epon@
 alarm                    - setting system alarm
 best-sys                 - configure sys information
 epon-workmode            - configure EPON working-mode
 ethernet-ring            - configure rapid ring
 igmp-snooping            - configure IGMP Snooping
 interface                - interface type
 ipconfig                 - configure the system IP address
 logout                   - exit the CLI system
 mac-address-table        - ctrl-card dynamic mac address table management
 mirror                   - configure switch mirror
 onu-auth                 - configure authentication mode for Olt
 ping                     - net ping
 port-isolate-group       - create port-isolate-group, you must enable port-isolate-mode for group
 rmon                     - configure RMON
 rstp                     - rapid spanning tree protocol configuration
```

[C-Data FD11XX series OLT version information and command line style]

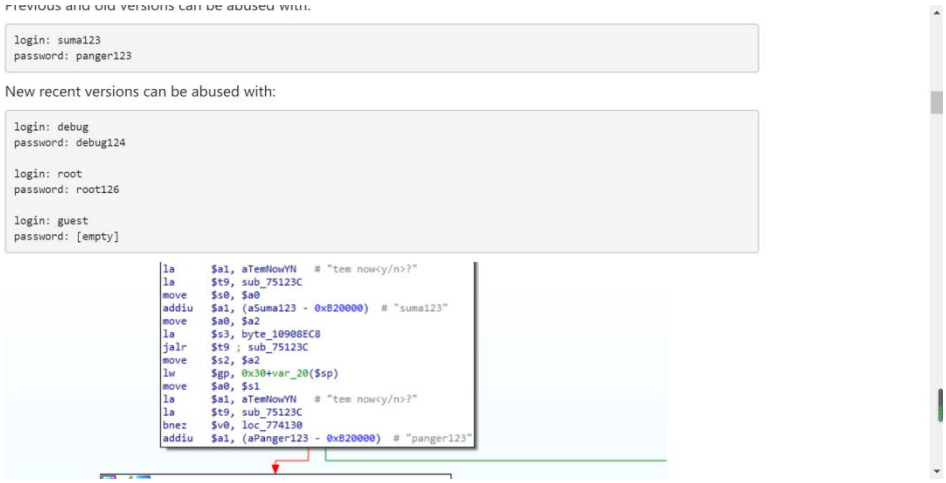
```
$ telnet [ip]
**********************************************************************
        Command Line Interface for EPON System
                Hardware Ver:  V3.2
                Software Ver:  2.4.04_001
                Created Time:  Nov 27 2017 10:38:49
    Copyright (c) 2006-2015 All rights reserved.
**********************************************************************
Username:root
Password:root126
epon#
-------------------------------------------------
  Local Configuration Command
-------------------------------------------------
 acl                      - Create ACL(s)
 acl-del                  - Delete ACL(s)
 auth                     - configure authentication mode for Olt
 btv                      - btv
 cdt-sys                  - configure sys information
 dhcp-snooping            - configure DHCP Snooping
 exec-timeout             - set a timeout value
 igmp                     - configure IGMP Snooping
 mac-address              - ctrl-card dynamic mac address table management
 mirror                   - configure switch mirror
 multicast-vlan           - multicast-vlan <mvlan>
 no                       - no
 olt                      - configure OLT
 reset                    - reset the values
 rmon                     - configure RMON
 rstp                     - rapid spanning tree protocol configuration
```

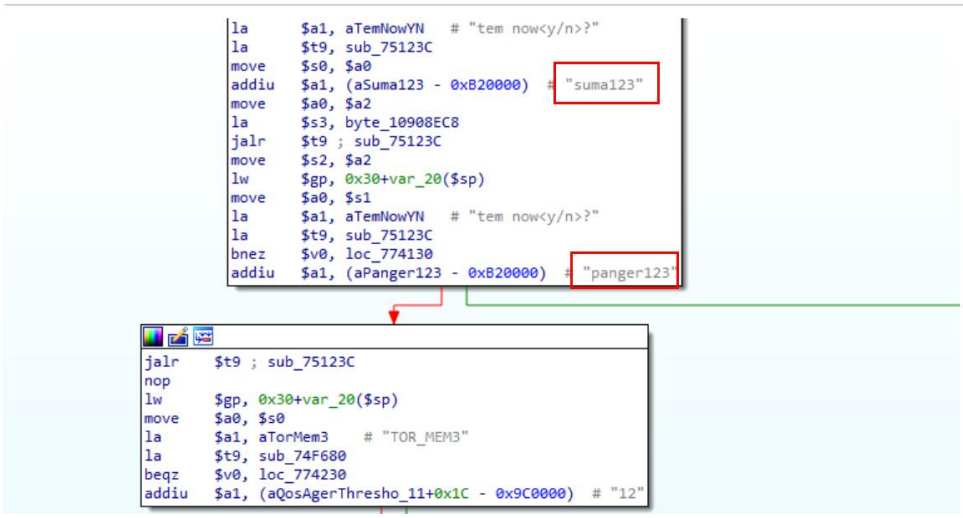
Если вы используете учетную запись panger123 / suma123, вы никогда не сможете получить доступ к C-Data OLT. На следующем рисунке показан информационный перехват неудачной попытки входа в C-Data OLT с учетной записью panger123 / suma123.

```
**********************************************************************
      Command Line Interface for EPON System
            Hardware Ver:  V3.1
            Software Ver:  2.4.05_000
            Created Time:  May 17 2018 11:16:52
   Copyright (c) 2006-2015 All rights reserved.
**********************************************************************
Username:panger123
Password:suma123
User name or password invalid!

Username:
```

В этой статье анализируется проблема, касающаяся процесса аутентификации с использованием жестко закодированных учетных данных. Демонстрация показывает, что мы заходим в bcm-оболочку OLT и получаем ключевую информацию о OLT методом telnet. Вся необходимая информация поступает из реплики, а не из OLT C-Data. На скриншотах информация об учетной записи и пароле, помеченная красным, - это подделка.





Введение в несколько учетных записей заводских настроек

1. Следующие две учетные записи и пароли для входа в telnet, упомянутые в этой статье, фактически используются в OLT первого поколения C-Data (OLT, начиная с FD11XX):

OLT telnet account 1: debug/debug124

OLT telnet account 2: root/root126

Эта учетная запись и пароль в основном используются C-Data для помощи клиентам в устранении проблем и написании производственных параметров. (Информация о MAC-адресе OLT и информация о SN и т. Д.)

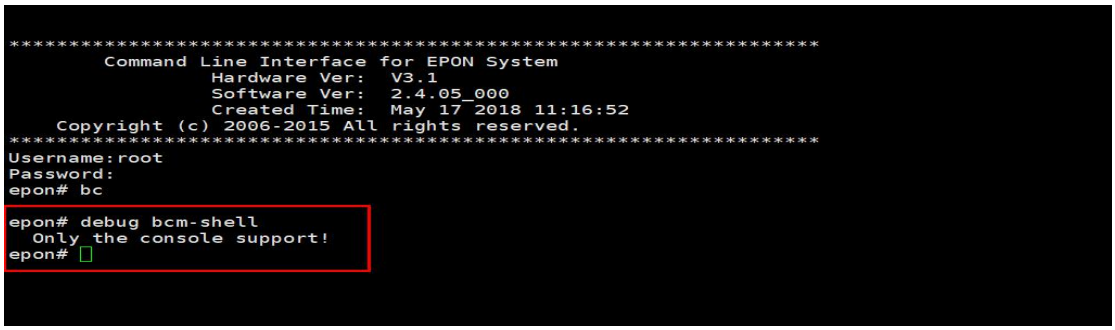
Учетная запись должна быть успешно подключена к порту CONSOLE с помощью локальной последовательной линии на OLT, а затем может войти в режим OLT bcm-shell для изменения и просмотра ключевой информации OLT. Использовать эту учетную запись в режиме OLT TELENT мы можем только введите CLI устройства, не может войти в OLT bcm-shell, изменить ключевую информацию OLT.

Если злоумышленники хотят войти в режим bcm-shell OLT, чтобы получить информацию о конфиденциальности устройства или внедрить вредоносные программы в OLT, они должны войти в OLT, напрямую подключив линию последовательного порта компьютера. Таким образом, удаленные злоумышленники ни в коем случае не могут использовать эти две учетные записи для атаки.

Таким образом, не существует такой ситуации, как «Backdoor Access with telnet».

Кроме того, что касается этих двух учетных записей, C-Data раскрыла нужным клиентам без бронирования. Обычное использование клиентов происходит, когда им нужно изменить MAC-адрес.

[На следующем рисунке показано, как выполнить удаленный вход в C-Data OLT с помощью debug / debug124 и root / root126, и как попытаться войти в приглашение режима оболочки. Кроме того, приглашение OLT поддерживает ввод bcm-shell только при прямом подключении к CONSOLE.]



Другой сценарий использования debug / debug124 и root / root126 - это когда C-Data предоставляет удаленную техническую поддержку по запросу клиента. Весь удаленный доступ C-Data получил согласие клиента после консультации с клиентами. При работе оператору необходимо удаленно войти на компьютер клиента, затем войти на устройство, используя локальные последовательные порты этих двух учетных записей, и таким образом работать с клиентом для анализа местоположения сетевых проблем. Технические специалисты Заказчика будут участвовать и контролировать процесс технического обслуживания на протяжении всего процесса.

Что касается того, существует ли проблема, когда злоумышленник входит в CLI, используя эти две учетные записи через TELNET, а затем изменяет конфигурацию OLT, что приводит к проблемам с сетевой безопасностью, мы дополнительно объясним это позже в политике безопасности.

OLT telnet Account3：guest/[empty]

Учетная запись и пароль являются учетной записью заводской конфигурации по умолчанию, которая может проверять только некоторую основную информацию о OLT и не имеет полномочий для настройки какого-либо OLT. Пользователь может удалить или изменить учетную запись по мере необходимости при ее использовании.

2. Решение. Поскольку OLT серии FD11XX является первым поколением моделей C-Data OLT, правила учетной записи и пароля которого полностью не учтены. Пароль по умолчанию является фиксированным и слишком простым, что может быть использовано преступниками. C-Data немедленно обновит и выпустит версию программного обеспечения этого продукта OLT. В последней версии отладочная учетная запись больше не будет принимать общий фиксированный пароль, а пароль будет генерироваться специальным средством генерации пароля в соответствии с уникальным идентификационным кодом, привязанным к устройству. Если информация об уникальном идентификационном коде устройства или инструмента

генерации пароля отсутствует, пароль получить невозможно.

Больше о Secure Cryptographic

Для других моделей OLT C-Data (OLT с именем FD15XX, FD16XX, FD12XX, FD8000) проблема «Backdoor Access with telnet» не существует, поскольку эти OLT используют более безопасный криптографический механизм. По умолчанию устройство настроено с несколькими общими учетными записями, включая root / admin, admin / admin и guest / guest, которые могут использоваться клиентами для первоначальной настройки OLT. Клиенты должны создавать, удалять и изменять учетную запись и пароль устройства в соответствии со своими политиками безопасности при использовании устройства. Мы не рекомендуем использовать заводские настройки по умолчанию для имени пользователя и пароля в операционной сети.

Устройство сохраняет отладочную учетную запись для помощи клиентам в отладке и решении проблем, и эта учетная запись также может использоваться клиентом для поиска забытого пароля, когда они забывают пароль для входа в OLT. Однако учетная запись больше не использует общий пароль, и пароль рассчитывается и генерируется в соответствии с уникальной идентификационной информацией OLT клиента. Только когда клиент предоставляет информацию об уникальном идентификационном коде в сочетании со специальным инструментом генерации пароля, пароль может быть сгенерирован. Пароль каждого OLT индивидуален, что позволит лучше обеспечить безопасность устройства.

The Requirement of WEB Login Management

Имя пользователя и пароль, отображаемые в этой статье, на самом деле нужны многим пользователям. Учетная запись и пароль - это имя пользователя и пароль для входа в веб-интерфейс управления OLT. Поскольку многие отзывы клиентов о том, что некоторые из их младшего обслуживающего персонала могут легко забыть имя пользователя и пароль веб-интерфейса управления OLT, и надеются, что менеджеры более высокого уровня смогут запросить имя пользователя и пароль веб-узла через OLT CLI, мы предоставляем эту команду по адресу запрос клиента, чтобы клиенты могли сами проверить имя пользователя и пароль для входа в сеть через командную строку. Мы считаем, что клиент может сформулировать эффективную систему управления безопасностью, правильно управлять использованием имен пользователей и паролей, чтобы избежать риска использования этой команды.

Details - Credentials infoleak and credentials in clear-text (telnet)

For this part, we suppose the attacker has a working CLI access (which can be achieved using Backdoor access with telnet).

It is possible to extract administrator credentials by running this command in the CLI:

```
epon# show system infor
Web Server
  Version          : V1.2.0
  BuildTime        : 19-04-23
  Administrator    : LOGIN_CLEAR_TEXT
  Password         : PASSWORD_CLEAR_TEXT
```

Security strategies and suggestions

1. В статье представлены несколько схем, которые можно использовать для атаки на C-Data OLT после знания учетной записи и пароля «Backdoor Access с telnet» в C-Data с точки зрения угроз безопасности сети. C-Data считает, что большинство клиентов имеют ряд мер, подходящих для их собственной защиты от кибератак. Далее будут перечислены общие меры защиты от кибератак на стороне клиента. Эти меры могут защитить OLT от следующих средств атаки, упомянутых в статье:

* Escape-оболочка с правами root

* Pre-Auth Remote DoS

* Информация об утечке информации и учетные данные в виде открытого текста (HTTP)

* Слабый алгоритм шифрования

* Небезопасные интерфейсы управления

Стратегия защиты 1: В общем планировании сети все VLAN управления OLT и сервисные VLAN на стороне клиента различны. Если управляющая VLAN, используемая злоумышленником, неверна, этот тип планирования делает невозможным доступ к оборудованию OLT со стороны сети OLT (восходящая линия связи) или со стороны пользователя (нисходящая линия связи с ONU).

```
 who                    - Display users currently logged in
epon# system ipconfig
-------------------------------------------------
  Local Configuration Command
-------------------------------------------------
 gateway                - configure the gateway
 inband                 - configure the inband IP address
 mgmt-vlan              - management vlan configuration
 outband                - configure the outband IP address
epon# system ipconfig mgmt-vlan
 <vid>                  - 1-4094
epon# system ipconfig mgmt-vlan 100
-------------------------------------------------
  Local Configuration Command
-------------------------------------------------
 <cr>                   - Please press ENTER to execute command
epon# system ipconfig mgmt-vlan 100
```

Стратегия защиты 2: OLT используется в качестве устройства уровня доступа. Для многих малых и средних интернет-провайдеров OLT обычно развертывается во внутренней сети. Когда интрасеть переходит в общедоступную сеть, она проходит через маршрутизатор или брандмауэр. Такие службы, как telnet и http, отключены на маршрутизаторе и оборудовании межсетевого экрана; Те, кто получает доступ к OLT, являются сотрудниками, которые имеют доступ к OLT во внутренней сети клиента; Действительно, если есть другой персонал, которому необходимо получить доступ к устройству OLT во внутренней сети через общедоступную сеть, ему необходимо выполнить переадресацию портов на маршрутизаторе или брандмауэре, и только клиент знает правила переадресации, поэтому злоумышленнику будет сложно получить информацию и провести атаку.

Стратегия защиты 3: OLT C-Data разработала множество стратегий управления, которые устанавливаются самими заказчиками, и она может полностью предотвратить проникновение сетевых атак злоумышленников на устройство:

OLT настройка стратегии 1: Он может контролироваться системой контроля доступа OLT, чтобы разрешить определенным IP-адресам или mac доступ к устройству OLT, настроенному пользователем, и совершенно неизвестен другим.

```
epon# system access-control
-------------------------------------------------
  Local Configuration Command
-------------------------------------------------
 access-ip-add          - add access ip address
 access-ip-del          - del access ip address
 access-mac-add         - add access mac address
 access-mac-del         - del access mac address
 admin                  - enable or disable access control
epon# system access-control
```

Стратегия конфигурирования OLT 2: Входной доступ к OLT может быть включен или отключен клиентом. Клиенты могут отключить внутреннее управление и использовать внешнее управление. В этом случае управление устройством достигается через выделенный канал управления, отделенный от бизнес-данных, таким образом, безопасность сети выше.

```
epon# system aux-port-admin
 <admin>                - <enable|disable>
epon# system aux-port-admin
```

Стратегия настройки OLT 3: Порт веб-доступа OLT может быть изменен пользователем и может быть закрыт и открыт клиентом.

```
epon# system web
-------------------------------------------------
  Local Configuration Command
-------------------------------------------------
 default-port          - default servicePort 80
 disable               - disable web-sever
 enable                - enable web-sever
 port                  - server port
epon# system web port
 <port>                - <8000-9999>
epon# system web port
```

Стратегия конфигурирования OLT 4: OLT может быть сконфигурирована с идеальной функцией acl для предотвращения легкой атаки на устройство.

```
olt 1
acl 4 rule 4 up match "dst-ip=190.115.18.238" action "fwd=deny "
acl 6 rule 4 up match "dst-port=422" action "fwd=deny "
exit
olt 2
acl 4 rule 4 up match "dst-ip=190.115.18.238" action "fwd=deny "
acl 6 rule 4 up match "dst-port=422" action "fwd=deny "
exit
olt 3
acl 4 rule 4 up match "dst-ip=190.115.18.238" action "fwd=deny "
acl 6 rule 4 up match "dst-port=422" action "fwd=deny "
exit
olt 4
acl 4 rule 4 up match "dst-ip=190.115.18.238" action "fwd=deny "
acl 6 rule 4 up match "dst-port=422" action "fwd=deny "
exit
```

```
epon# acl
acl                 acl-del
epon# acl
 <id>                 - ACL ID:
                        <1-2000>basic acl,match condition:src-ip;
                        <2001-5000>advanced acl,match condition:dscp|dst-ip|
                        dst-port|ip-protocol|src-ip|src-port|tos;
                        <5001-8000>link acl,match condition:
                        dst-mac|eth-type|src-mac|vlan;
                        <8001-10000>user acl, not support now.
epon# acl
```

Заключение

Статья Пьера Кима и Александра Торреса суммировала в деталях и серьезно тестирует устройство C-Data с точки зрения уязвимостей безопасности. Первоначальная цель первоначальной статьи заключалась в том, чтобы сообщить об уязвимостях системы безопасности в устройстве, чтобы технические специалисты и пользователи замечали угрозы безопасности и принимали эффективные меры безопасности, а не значение «черного хода устройства OLT», когда средства массовой информации передавали распространение, и не должны интерпретировать как C-Data намеренно оставил бэкдор на продукте. C-Data ожидает, что продукты предоставят клиентам лучший опыт и сделают его более удобным для использования устройства. C-Data имеет возможность помочь клиентам лучше разработать стратегии защиты в кибербезопасности. C-Data также призывает все стороны выдвигать

разумные предложения, чтобы устройство C-Data могло уделять больше внимания вопросам безопасности клиентов и путанице при использовании устройства с целью обеспечения удобства и практичности для клиентов. Спасибо!

Shenzhen C-Data Technology Co., Ltd

Отдел Маркентинг C-DATA

pan@cdatatec.com