Security Notification – ConneXium Managed Switch

17-Feb-2016

Overview

Schneider Electric® ConneXium Switches contain a password synchronization feature that syncs the switch passwords with the SNMPv1/v2 communities. If this feature is enabled the communities may give attackers the ability to recover the switch passwords.

Vulnerability Overview

For ConneXium “Basic Managed” “Standard Managed” and “Extended Managed” switches, by default, the switch “user” and “admin” passwords are used to construct corresponding SNMPv1/v2 read-only and read-write community strings that allow remote management of the switch configuration

Product(s) Affected

ConneXium “Basic Managed” “Standard Managed” and “Extended Managed” switches with the following commercial references and firmware versions:

TCSESB083F23F0, TCSESB083F2CU0, TCSESB093F2CU0	Firmware Versions 5.36 and below
TCSESM043F23F0, TCSESM043F2CU0, TCSESM043F2CS0, TCSESM043F1CU0, TCSESM043F1CS0, TCSESM083F23F0, TCSESM083F2CU0, TCSESM083F2CS0, TCSESM083F1CU0, TCSESM083F1CS0, TCSESM103F23G0, TCSESM103F2LG0, TCSESM163F23F0, TCSESM163F2CU0, TCSESM163F2CS0, TCSESM243F2CU0	Firmware Versions 08.09 and below
TCSESM083F23F1, TCSESM063F2CU1, TCSESM063F2CS1, TCSESM083F23F1C, TCSESM063F2CU1C, TCSESM063F2CS1C	Firmware Versions 08.09 and below

Vulnerability Details

As SNMPv1/v2 communication is sent unencrypted an attacker on the local network with the ability to sniff network traffic may be able to recover the passwords from the community strings if the switch is managed via SNMPv1/v2. An attacker may also be able to extract the community strings from a configuration file because they are stored in plain text.

An attacker on the local network may learn the switch administrator password from the SNMP community string, which is sent over the network in plaintext in SNMPv1 and SNMPv2Overall CVSS Score: 8.3

(AV:A/AC:L/Au:N/C:C/I:C/A:C/ E:F/RL:OF/RC:C/DP:ND/TD:M/CR:ND/IR:ND/AR:ND)

Mitigation

Disable the SNMP Password Sync feature and use SNMPv3

Affected users may disable the password sync feature on their devices. For more information, please see Refer to “Details on workaround for above mentioned vulnerabilities”. Users are also encouraged to use SNMPv3, which supports encrypted network traffic.

The next firmware update for all models will disable the password synchronization feature by default.

Details on workaround for above mentioned vulnerabilities:

Perform the following actions:

(1) Change the read and read/write passwords
(2) Set the SNMPv1/v2 communities to default values (see (A) for details)
(3) Disable SNMPv1/v2 globally (see (B) for details)
(4) Save the configuration on the device

Please note: Step (2) must be performed every time the password is changed.

Detailed instructions:

(A) Set the SNMPv1/v2 communities to default values

Over the GUI:

- Open the “*SNMPv1/v2 Access*” dialog in the web interface and set the password for the “*readOnly*” Access Mode to “*public*” and the password for the “*readWrite*” Access Mode to “*private*”. This can also be set with the MultiConfig function of Industrial HiVision.

Over the CLI:

- execute the following commands in the configure mode:

```
(Config)#snmp-server community ro public
(Config)#snmp-server community rw private
```

(B) Disable SNMPv1/v2 globally

Over the GUI:

• disable the checkbox “*SNMPv1 enabled*” and “*SNMPv2 enabled*” in the “*SNMPv1/v2 Access*” dialog of the web interface. This can also be set with the MultiConfig function of Industrial HiVision.

Over the CLI:

• execute the following commands in the configure mode:

```
(Config)#snmp-access version v1 disable
(Config)#snmp-access version v2 disable
```

For More Information

This document is intended to help provide an overview of the identified vulnerability and actions required to mitigate it. To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric representative. These organizations will be fully aware of the situation and can support you through the process.

For further information on vulnerabilities in Schneider Electric’s products, please visit Schneider Electric’s cybersecurity web page at http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

About Schneider Electric

As a global specialist in energy management with operations in more than 100 countries, Schneider Electric offers integrated solutions across multiple market segments, including leadership positions in Utilities & Infrastructures, Industries & Machine Manufacturers, Non-residential Buildings, Data Centers & Networks and in Residential.
www.schneider-electric.com