Important Security Notification – SNMPv3 Authentication Bypass

July 15, 2015

Schneider Electric® has become aware of a SNMPv3 Authentication vulnerability that may allow authentication bypass if specifically crafted packets are used.

The vulnerability detail:

Authentication for SNMPv3 is done using keyed Hash Message Authentication Code (HMAC), A cryptographic checksum over the SNMP message in combination with a secret key (derived from the user password). The HMAC and user name are transmitted within the packet. The device verifies the integrity and originator of the message by calculating a checksum over the received message with the secret key from its local user database. If the calculated HMAC and the one in the packet match, access is granted.

Omitting the HMAC by reducing the length to zero causes the implementation on the device to compare zero bytes HMAC. In this case access is granted.

This vulnerability was discovered during cyber security research both by an external researcher and by Schneider Electric internal investigations. We have no evidence that this vulnerability have been exploited.

Schneider Electric takes these vulnerabilities very seriously and we have devoted resources to immediately investigate and address these issues. We believe it is critical to consider the whole picture, including safety, security and reliability. Any patches/solutions/mitigations we release will be carefully tested to ensure that they can be deployed in a manner that is both safe and secure.

Details on products affected:

The following products are affected by this vulnerability:

1) The 22 ConneXium Ethernet Managed Switch products (TCSESM… series running firmware SV: 08.04 or lower).

TCSESM043F23F0	TCSESM103F23G0	TCSESM063F2CU1C
TCSESM043F1CU0	TCSESM103F2LG0	TCSESM063F2CS1C
TCSESM043F2CU0	TCSESM163F23F0	
TCSESM043F1CS0	TCSESM163F2CU0	
TCSESM043F2CS0	TCSESM163F2CS0	
TCSESM083F23F0	TCSESM243F2CU0	
TCSESM083F1CU0	TCSESM083F23F1	
TCSESN083F2CU0	TCSESM063F2CU1	
TCSESM083F1CS0	TCSESM063F2CS1	
TCSESM083F2CS0	TCSESM083F23F1C	

2) The 3 ConneXium Ethernet Basic Switch Products (TCSESB… series running firmware SV: 05.35 or lower).

TCSESB083F23F0
TCSESB083F2CU0
TCSESB093F2CU0

Details on workaround and planned fix dates for above mentioned vulnerabilities:

The following workarounds have been identified:

1) Enabling the privacy(encryption) option for all users will prevent the use of this vulnerability:
   a) To do that over the GUI, enable the check-box “Accept only encrypted requests” in the “Password/SNMP access” dialog of the web interface. This can be set with the multi-configuration function of ConneXium Network Manager.
   b) To do that over the CLI, execute the following commands in the configure mode:
   (config)#snmp-access version v3-encription readonly
   (config)#snmp-access version v3-encription readwrite
   c) Enabling this option can be performed without rebooting the device and therefore it can be activated without affecting the network.
2) An alternative workaround is to block all SNMP requests using the “Restricted Management Access” feature.

Schneider Electric is in process of updating ConneXium switch products to resolve this vulnerability through a firmware update. The updated firmware will be available on Schneider Electric web site. The fix for this vulnerability is contained in the following:

TCSESM…. Product series running firmware SV:08.09 or greater.

TCSESB … Product series running firmware SV: 05.36 or greater

General Recommendations

Schneider Electric has been designing industrial automation products for many years and recommends to its customers, industry best practices in the development and implementation of control systems. This recommendation includes a Defense in Depth approach to secure an Industrial Control System. This approach places the PLCs behind one or more firewalls to restrict access to authorized personnel and protocols only. The location of the firewalls is decided based on how large the trusted zone is required to be. Please read the following document for more detailed information:

http://download.schneider-electric.com/files?p_File_Id=25779912&p_File_Name=Cyber-Security-STN-v2-Aug-2012.pdf

For Resolution 207869 click link below:
http://download.schneider-electric.com/files?p_File_Id=25575596&p_File_Name=Res207869.pdf

Acknowledgments

Support CVSS Scoring

CVSS scores are a standard way of ranking vulnerabilities and are provided for reference based on a typical control system, they should be adapted by individual users as required.

Overview

SNMPv3 HMAC verification in (1) Net-SNMP 5.2.x before 5.2.4.1, 5.3.x before 5.3.2.1, and 5.4.x before 5.4.1.1; (2) UCD-SNMP; (3) eCos; (4) Juniper Session and Resource Control (SRC) C-series 1.0.0 through 2.0.0; (5) NetApp (aka Network Appliance) Data ONTAP 7.3RC1 and 7.3RC2; (6) SNMP Research before 16.2; (7) multiple Cisco IOS, CatOS, ACE, and Nexus products; (8) Ingate Firewall 3.1.0 and later and SIParator 3.1.0 and later; (9) HP OpenView SNMP Emanate Master Agent 15.x; and possibly other products relies on the client to specify the HMAC length, which makes it easier for remote attackers to bypass SNMP authentication via a length value of 1, which only checks the first byte.

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C) (legend)

Impact Subscore: 10.0

Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Low

Authentication: Not required to exploit

Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service