Hirschmann "Classic Platform" switches reveal administrator password in SNMP community string by default

Vulnerability Note VU#507216

Original Release Date: 2016-02-16 | Last Revised: 2016-11-09

Overview

Hirschmann "Classic Platform" switches contain a password sync feature that syncs the switch administrator password with the SNMP community password, exposing the administrator password to attackers on the local network.

Description

ABOUT VULNERABILITY NOTES

CONTACT US ABOUT THIS VULNERABILITY

PROVIDE A VENDOR STATEMENT

CWE-257: Storing Passwords in a Recoverable Format

For all Hirschmann (part of Belden) "Classic Platform" switches (which includes the MACH series workgroup switches, among others), by default, the switch administrator password is used to construct an SNMP community string that allows remote management of some switch configuration. Attackers on the local network with the ability to sniff network traffic may be able to recover the administrator password from the community string.

Belden has released security advisory BSECV-2016-2 which describes this issue in more detail.

Impact

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 SNMPv2.

Solution

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 Belden security advisory BSECV-2016-2. Users are also encouraged to use SNMPv3, which supports encrypted network traffic.

According to Hirschmann, the password sync feature was enabled by default to aid in network setup during the transition from SNMPv1/v2 to SNMPv3. Hirschmann has committed to disabling the password sync feature by default in future devices and firmware now that SNMPv3 is the default on their products.

Vendor Information

Filter by status: All

Filter by content:

Additional information available

Sort by: Status

Expand all

Belden	Affected
Yokogawa Electric Corporation	Affected

CVSS Metrics

Group	Score	Vector
Base	8.3	AV:A/AC:L/Au:N/C:C/I:C/A:C
Temporal	6.9	E:F/RL:OF/RC:C
Environmental	5.2	CDP:ND/TD:M/CR:ND/IR:ND/AR:ND

References

- **https://www.belden.com/resourcecenter/security/upload/Belden_Security_Advisory_BSECV-2016-2_1v0.pdf**
- **http://www.hirschmann.com/en/Hirschmann_Produkte/Industrial_Ethernet/Workgroup-Switches_MACH100/index.phtml**

Acknowledgements

Thanks to Mark Jaques for reporting this vulnerability.

This document was written by Garret Wassermann.

Other Information

CVE IDs: None

Date Public:	2016-02-16
Date First Published:	2016-02-16
Date Last Updated:	2016-11-09 21:38 UTC
Document Revision:	65

Sponsored by CISA.

Download PGP Key

Read CERT/CC Blog

Learn about Vulnerability Analysis

Carnegie Mellon University
Software Engineering
Institute
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
412-268-5800

Contact SEI

Contact CERT/CC

412-268-5800
cert@cert.org