SNMPv3 Authentication Bypass

Date: July 10, 2015
Version: 1.0
References: CVE-2008-0960

Executive Summary

The implementation of SNMPv3 contains a vulnerability that may allow authentication bypass if specially crafted packets are used.

Details

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.

Impact

This vulnerability allows attackers to read and modify any SNMPv3 object that can be accessed by the impersonated user. Attackers exploiting this vulnerability can view and modify the configuration of these devices.

Affected Products

Brand	Platform	Product	Version
Hirschmann	Classic L2E, L2P, L3E and L3P	RS, RSR, MACH100, MACH1000, MACH4000, MS, OCTOPUS	08.0.08 and lower
	Classic L2B	RSB	05.3.05 and lower
	HiOS	RSP, EES	01.1.02 and lower
GarrettCom	MNS	6K, 10K	4.5.7 and lower
	RX	5RX, 10RX	3.1.3 and lower

Solution

Update affected products to the following release that resolves this issue.

Brand	Platform	Version	Links
Hirschmann	Classic L2E, L2P, L3E and L3P	08.0.09 or higher	[3]
	Classic L2B	05.3.06 or higher	[4]
	HiOS	02.0.00 or higher	[5]
GarrettCom	MNS	4.5.8 or higher	[6]
	RX	3.1.4 or higher	[7]

The following workarounds can be used for products with Classic Software L2P and higher:

(1) Enabling the privacy (encryption) option for all users will prevent the use of this vulnerability:

- 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 also be set with the multi-configuration function of Industrial HiVision.
- To do that over the CLI execute the following commands in the configure mode:
  (config) #snmp-access version v3-encryption readonly
  (config) #snmp-access version v3-encryption readwrite
- 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.

On products with HiOS software the encryption is enabled by default. No action is necessary if encryption was not disabled.

For Help or Feedback

To view all Belden Security Advisories and Bulletins or to report suspected security vulnerabilities, go to https://www.belden.com/security.
For technical support and other requests, please visit https://hirschmann-support.belden.eu.com and https://garrettcom-support.belden.eu.com.

Related Links

- [1] Vulnerability Note VU#878044:
  https://www.kb.cert.org/vuls/id/878044
- [2] National Vulnerability Database:
  http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0960
- [3] Download link for Software Release 08.0:
  http://www.e-catalog.beldensolutions.com/link/57078-24455-278205-377857-374457/en/conf/0
- [4] Link to the Hirschmann support portal:
  https://hirschmann-support.belden.eu.com
- [5] Download link for HiOS Release 04.0:
  http://www.e-catalog.beldensolutions.com/link/57078-24455-278205-377857-412440/en/conf/0
- [6] Download link for MNS Release 4.5.8:
  http://www.garrettcom.com/techsupport/sw_downloads.htm
- [7] Please contact the GarrettCom technical support:
  gcisupport@belden.com

Disclaimer

Revisions

V1.0 (July 10, 2015): Bulletin created.