Passwords Synchronization with SNMP v1/v2 Communities

Date: December 19, 2016
Version: 1.1
References: VU#507216

Executive Summary

Hirschmann “Classic Platform” 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.

Details

For all Hirschmann “Classic Platform” 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. As SNMPv1/v2 communication is sent unencrypted, an attacker who is on the local network and has 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.

Impact

An attacker on the local network may learn the switch read-only and read-write passwords from the SNMP community strings and thereby achieve full administration access to the switch.

Affected Products

Brand	Platform	Product	Version
Hirschmann	Classic L2E, L2P, L3E and L3P	RS, RSR, MACH100, MACH1000, MACH4000, MS, OCTOPUS	09.0.05 and lower
	Classic L2B	RSB	05.3.06 and lower

Suggested Actions

For devices with versions 09.0.00 and higher perform the following actions:

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

For devices with versions lower than 09.0.00 perform the following actions:

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

Please note: For devices running a version lower than 09.0.00 step (2) must be performed every time the password is changed.

Detailed instructions:

(A) Disable the SNMP password synchronization feature
Over the GUI:
- Disable the checkbox "*Synchronize passwords to v1/v2 community*" in the "*Password/SNMP access*" dialog of the web interface.
- Disable the checkbox "*Synchronize community to v3 password*" in the "*SNMPv1/v2 Access*" dialog of the web interface.

Over the CLI:
- Execute the following commands in the configure mode:

```
(config)# no snmp sync v3-to-community
(config)# no snmp sync community-to-v3
```

(B) 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
```

(C) 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
```

Solution

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

Brand	Platform	Version	Links
Hirschmann	Classic L2E, L2P, L3E and L3P	09.0.06 or higher	[2]
	Classic L2B	05.3.07 or higher	[3]

After updating and rebooting the device please perform the suggested actions defined above.

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.

Related Links

- [1] Vulnerability Note VU#507216: https://www.kb.cert.org/vuls/id/507216
- [2] The Classic Switch Software (Release 9): http://www.hirschmann.com/en/Hirschmann_Produkte/Industrial_Ethernet/Software/Software_Platforms/Switch-Classic-Software/index.phtml

- [3] Basic Switches – Download: https://www.e-catalog.beldensolutions.com/link/57078-24455-49854-84128-399555/en/RSB20-0900VVM2SAABHH/0-0

Disclaimer

Revisions

V1.0 (February 16, 2016): Advisory published.
V1.1 (December 19, 2016): Converted to bulletin format.