Identical SSH and SSL default keys in HiLCOS products

Date: December 11, 2015
Version: 1.0
References: VU#566724

Executive Summary

HiLCOS products were delivered with identical keys for SSH and SSL. **If these keys are not replaced by the customer**, the encrypted SSL (HTTPS) and SSH device management protocols can – under certain conditions – be deciphered by man-in-the-middle attacks.

Belden recommends that its customers upgrade to HiLCOS version 9.10 as defined in the solution below.

Details

For details please see the Vulnerability Notes Database entry VU#566724.

Impact

According to current knowledge, this vulnerability has not yet been exploited for an attack. Theoretically, a remote, unauthenticated attacker may be able to carry out impersonation or man-in-the-middle attacks, resulting in the exposure of sensitive information.

Affected Products

With identical default SSH keys:
Devices delivered from the factory with one of the affected firmware versions and no individual keys were generated.

Brand	Product Line / Platform	Product	Version
Hirschmann	HiLCOS	OpenBAT	8.60
		WLC, BAT300, BAT54	8.52 and lower

With identical default SSL keys:
Devices running one of the affected firmware versions and no individual certificate installed.

Brand	Product Line / Platform	Product	Version
Hirschmann	HiLCOS	OpenBAT, WLC	9.00* and lower
		BAT300, BAT54	8.80 and lower

** for 9.00-RU1 unique keys were inserted during production.*

Solution

Generation of unique SSH keys after configuration reset is supported in the following releases:

Brand	Products	Version	Links
Hirschmann	OpenBAT, WLC BAT300, BAT54**	8.80 and higher	Hirschmann Support Portal [1]

*** for BAT54Client no update is available. Please use the workaround described below after every configuration reset.*

If the device in question has been delivered from the factory with an older firmware version, the keys are not automatically replaced by individual keys. Please follow the steps described as “Workaround SSH” below.

Generation of unique SSL keys after configuration reset is supported in the following releases:

Brand	Product Line / Platform	Version	Links
Hirschmann	OpenBAT, WLC	9.10 and higher	Hirschmann Support Portal [1]

Workaround for SSH
Unique SSH keys can be created on the HiLCOS command line interface in HiLCOS 8.00 and higher software versions. Please execute the following commands:

```
sshkeygen -t rsa -b 2048 -f /minifs/ssh_rsakey
sshkeygen -t dsa -b 1024 -f /minifs/ssh_dsakey
```

For detailed information, please refer to the following section of the corresponding Configuration and Administration Guide [2] related to the device:

- Section *"Automatic generation of device-specific SSH keys"*

Workaround for SSL
An individual SSL public/private key pair with associated certificate can be created externally from a public or private certificate authority. This can be installed in the HiLCOS device using a PKCS-12 container. For detailed instructions, please refer to the following two sections in the corresponding Configuration and Administration Guide [2] related to the device:

- The creation of a PKCS-12 container including an individual device certificate is described in section *"Creating certificates with OpenSSL / Issuing a certificate for users or devices"*
- The upload of the created PKCS-12 container is described in section: *"Loading certificates into the Hirschmann device"*

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] Link to the Hirschmann support portal
  https://hirschmann-support.belden.eu.com
- [2] Link to Hirschmann wireless products, software and manuals
  https://www.e-catalog.beldensolutions.com/link/57078-24455-49859-24497/en/conf/0-0

Disclaimer

Revisions

V1.0 (December 11, 2015): Bulletin published.