GECKO authentication bypass

Date: March 7, 2016
Version: 1.0

Executive Summary

The GECKO Lite Managed Switch contains a flaw that allows unauthorized users to upload official firmware images. Users are advised to update to the software version 02.0.00.

Details

The GECKO contains a flaw that allows unauthorized users to upload firmware images. This allows attackers to reach the management interface (the HTTP server) of the device to upload valid firmware images.

Impact

A downgrade could cause instabilities from issues present in previous versions.

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	Lite Managed Switches	GECKO	01.0.00, 01.0.01

Suggested Actions

It is recommended that users update to the version 02.0.00.

As a work-around, it is possible to prevent this system flaw from being exploited by shielding the GECKO web interface from public access. The device should only be connected to an intranet and the management interface should not be exposed to the public. If necessary, the device should be placed behind a firewall that implements this kind of restriction.

Solution

Users are advised to update to the following version:

Brand	Product Line / Platform	Product	Version
Hirschmann	Lite Managed Switches	GECKO	02.0.00

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.

Disclaimer

Revisions

V1.0 (March 7, 2016): Bulletin published.