Possible Request Forgery Vulnerabilities for GECKO Devices

Date: April 7, 2017
Version: 1.0
References: ICSA-17-026-02A

Executive Summary

The web interface of the GECKO does not verify that requests originate from the user. An administrator could be tricked into opening a URI that then, for example, modifies the GECKO configuration. Additionally, such a URI could also instruct the device to make a request to another server and, for example, download and install a certificate file. Customers are advised to update to the software version 02.0.01 and to not access URIs from outside sources while administrating their device(s).

Details

The web interface of the GECKO is susceptible to a cross-site request forgery vulnerability. It does not verify that a request originates from an authenticated user. An administrator could therefore be tricked into opening a URI that modifies the configuration of the device, for example, changing the administrator password. Additionally, this may also be used for a server-side request forgery as some particular URIs cause the device to initiate a request to another server, for example, to download and install a certificate file.
Only administrators that access URIs from outside sources while administrating a GECKO device are vulnerable and only if the attacker has knowledge about the address or DNS name of the GECKO and can trick the administrator into opening a crafted link.

Impact

Attackers may trick administrators into changing the configuration of the device.

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	Lite Managed	GECKO	02.0.00 and lower

Suggested Actions

It is recommended that customers update to the version 02.0.01 or later.

We advise customers to not access URIs from outside sources while they are logged in to a GECKO device with administrator privileges.

Solution

Customers are advised to update to the following version:

Brand	Product Line / Platform	Product	Version
Hirschmann	Lite Managed	GECKO	02.0.01 or later

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.

Acknowledgments

Belden thanks Davy Douhine from RandoriSec for working with us in this context to help protect customers.

Related Links

- [1] Firmware Download GECKO: https://www.e-catalog.beldensolutions.com/link/57078-24455-402707-402708/en/conf/0

Disclaimer

Revisions

V1.0 (April 7, 2017): Bulletin published.