Security Advisory

2022-06-13-01 Security Advisory.pdf

Metadaten

Published: 13.06.2022
Version:1.0

Affected Products:

Products	Affected Firmware Versions	Patched Firmware Version	Recommended Firmware Version
ID ISC.LR2500-A	All	n.a.	n.a.
ID ISC.LRM2500-A	All	n.a.	n.a.
ID ISC.LRU3000-EU	All	n.a.	n.a.
ID ISC.LRU3000-FCC	All	n.a.	n.a.
ID ISC.LRU3500-EU	All	n.a.	n.a.
ID ISC.LRU3500-FCC	All	n.a.	n.a.

Summary:

FEIG is aware of potential vulnerabilities and attack scenarios associated with the Mirai malware and Linux-based RFID read/write devices. The Mirai malware can turn Linux-based networked devices into remotely controlled bots that can be used as part of a botnet in large-scale network attacks. Mirai malware infiltrates via enabled services, nests in the target device and launches its attacks. Mirai cyclically scans the network for IoT devices and attempts to log in to the devices with default usernames and passwords and then infect them. Most common for Mirai are Denial-of-Service attacks.

Recommended immediate actions:

Remove the reader from the network and perform a firmware update. This will remove the corrupted code from the flash and restore it to its original state. Then observe the preventive measures below.

Preventive protection:

a) Disable unused services like TELNET, SSH, web server, FTP server and perform a reboot
b) Changing the default user names and passwords
c) Operate the reader only behind a firewall and do not open a port from the reader to the Internet via the firewall.

Disclaimer