Background

NETLINK™ is the patented remote monitoring Network Communications Module from LifeSafety Power, which after independent evaluation and assessment, has demonstrated proven system interfaces, instrumentation, and infrastructure safeguards to prevent surreptitious attacks to networked power solutions.

NOTE - For the highest cybersecurity protection, always update all NetLink devices to the latest firmware revision. The latest released firmware revision may be downloaded at: lifesafetypower.com/support/software-firmware-downloads

Cybersecurity Protection Features

» User login to Netlink modules are logged
» Multi-level user accounts (Guest, Manager, Admin)
» Multi-level passwords:
  - Salted hashed password
  - Password supports special characters
  - Repeated wrong password with programmable lockout duration
  - Minimum password length and complexity requirement
» Cross-Site Request Forgery (CSRF) protection with random token
» Use TLS 1.2 protocol and new cipher suites.
» Support pkcs12 CA certificate download
» Certificate logging
» Upgraded to latest Apache web server
» User option to put in latest ciphersuite for Apache SSL/TLS configure file
» Protection against DoS or DDoS attack or brute force attack
» Rules added to iptables filter input chains to prevent syn-flood, DDoS, CC attack
» Updated kernel to 3.1.0 and merged the net-firewall/conllimit package to be compatible with iptables “conllimit” function
» HTTPS ONLY mode disables non-SSL access
» Closed all unused ports
» SNMP version 1 & 2 for legacy, and version 3 for security
» Email encryption option
» Protection against Clickjacking
Application Recommendations for Cybersecurity

» Always change the default user name and passwords to a strong user name and password. We strongly suggest using the enhanced password option introduced in revision 8.071-28. Never leave the user name and password at the default “admin” once the NetLink is deployed on the network.

» Configure for secure web-based management. Use TLS (“https:”) whenever possible.

» Set the SSL option to “High” whenever possible.

» For SNMP alerts, use SNMP v3 with secured credentials whenever possible. Configure the PDU for SNMP traps.

Network Policy

» Device has static IP address

» If configured, device sends SMTP (tcp/25) traffic to a designated email alert server

» Device supports HTTPS (tcp/443 for inbound management)

» If configured, device supports SNMP and SNMP traps (udp/161,udp/162)

» If configured, device supports control traffic to vendor’s multi-device management solution

Enterprise Scanning

» The device should show up as HTTPS and SNMP (and possibly HTTP if not disabled)

Decommissioning

» Reset power distribution labeling

» Reset device to factory default

NETLINK Third Party Testing

NCCGroup and Smithee, Spelvin, Agnew & Plinge Inc., have both conducted independent cyber security assessments for infrastructure deployments, Internet-based solutions and network-attached devices. The NETLINK module was evaluated for cybersecurity-related features and design parameters and the methods with which NETLINK interfaces with email and the entire network infrastructure were found to present a cybersecurity posture appropriate for enterprise use.

LifeSafety Power, Inc.
Illinois USA
888-577-2898
technicalsupport@lifesafetypower.com