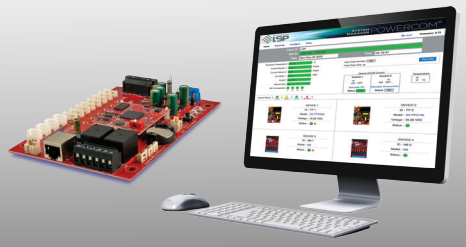
LIFESAFETY POWER NETLINK®

Cybersecurity Capabilities and Application Recommendations

03/ 2024



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.

Always update NetLink devices to the latest firmware revision for most up to date cybersecurity protection. Downloaded latest firmware at: https://www.lifesafetypower.com/knowledge-base/product-support/downloads

Cybersecurity Protection Features

- User login to Netlink modules are logged
- Minimum complexity password is enforced at initial login. Users are required to create a custom password at that time.
- Multi-level passwords:
  - Salted hashed password
  - Password supports special characters
  - Repeated wrong password with programmable lockout duration
  - Minimum password length and complexity requirement
- Firmware Anti-Rollback protection
- 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 4.1.15 and merged the net-firewall/connlimit package to be compatible with iptables “connlimit” function
- HTTPS ONLY mode disables non-SSL access
- Closed all unused ports to unwanted functionality
- Unused protocols and ports such as SNMP, ipv4 or ipv6 may be disabled

Cybersecurity Protection Features - continued

» SNMP version 1 & 2 for legacy, and version 3 for security
» Email encryption options including `plain', `cram-md5', `digest-md5', `scram-sha-1', `gssapi', `external', `login', and `ntlm'
» Protection against Clickjacking
» Software updated are cryptographically authenticated and provide anti-rollback features
» External inputs are validated and sanitized before evaluation or execution
» Encrypted firmware to increase the difficulty of extracting the firmware

Application Recommendations for Cybersecurity

» 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

Cobalt (12/2023 & 03/2024), NCCGroup (2017), and Smithee, Spelvin, Agnew & Plinge (2015), have all 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
Phoenix, AZ USA
888-577-2898
technicalsupport@lifesafetypower.com