



AN-X4-AB-DHRIO

Ethernet to Allen-Bradley DH+ / Remote I/O Gateway

Attack Surface Reduction (ASR)

Assessment Report

Prepared for: Quest Technical Solutions (QTS)

Product Marketed by: ProSoft Technology

Executive Summary

The QTS AN-X4-AB-DHRIO is a robust industrial gateway that enables seamless migration and integration between modern EtherNet/IP networks and legacy Allen-Bradley DH+ and RIO infrastructures. While the device historically presented a larger network attack surface typical of legacy industrial gateways (including management interfaces and protocol services with no native disable options), QTS has implemented targeted, configurable hardening measures.

These enhancements—delivered through microSD card-based modifications in specific firmware releases—allow operators to disable non-essential services such as SSH, web server, Modbus TCP, and the proprietary RIO configuration port. When combined with proper configuration (e.g., avoiding unnecessary HMI IP Aliases), the attack surface is significantly reduced, aligning with OT/ICS security best practices such as least-privilege networking and defense-in-depth.

This report assesses the pre- and post-mitigation attack surface, documents the new reduction options, and provides deployment recommendations. With these controls, the AN-X4-AB-DHRIO achieves a materially lower risk profile suitable for use in segmented industrial environments.

1. Product Overview

The AN-X4-AB-DHRIO gateway (produced by Quest Technical Solutions and marketed by ProSoft Technology) serves as a protocol bridge between Ethernet-based systems and legacy Allen-Bradley networks.

Key Functions:

- Supports DH+ and RIO operations via multiple firmware variants (e.g., AN-X4-AB-DHP for DH+, AN-X4-ABRIO-SCAN / AN-X4-ABRIO-ADPT for RIO).
- Built-in web server for diagnostics, configuration, firmware management, and monitoring.
- MicroSD card for firmware storage, configuration files, and now security hardening options.



- Supports EtherNet/IP, Client Server Protocol (CSP), Modbus TCP (in applicable firmware), and legacy HMI integration via IP aliasing.
- DIN-rail mountable, with standard RJ-45 Ethernet port.

The device is designed for phased modernization of legacy PLC-5, SLC, PanelView, and RIO-based systems without requiring PLC code changes. All configuration and firmware management occur via the microSD card and web interface (or direct card editing).

2. Default (Pre-Mitigation) Attack Surface

Prior to the security enhancements described below, the AN-X4-AB-DHRIO exposed several network services and protocols by default or under common configurations. This increased the potential for reconnaissance, unauthorized access, or exploitation in unsegmented or internet-facing industrial networks.

Historically Exposed Services and Ports:

- **Web Server** (TCP port 80 – standard browser-based configuration and diagnostics).
- **SSH** (TCP port 22 – previously always available for advanced/support access).
- **Modbus TCP** (TCP port 502 – in DHP firmware supporting Modbus client/server operations).
- **Allen-Bradley Client Server Protocol (CSP)** (TCP port 2222 – automatically exposed when Data Highway Plus HMI IP Aliases are configured).
- **Proprietary RIO Configuration Port** (TCP port 42889 – opened by RIO-SCAN and RIO-ADPT firmware for configuration tools).

Additional considerations:

- EtherNet/IP traffic (TCP/UDP ports 44818, 2222 for scheduled/unscheduled data) is inherent to the gateway's core function.
- No built-in authentication, encryption, or firewalling on management interfaces.
- MicroSD card access provided full control over firmware and config but required physical access.

This default surface was consistent with many legacy OT gateways but represented unnecessary exposure for modern security standards.

3. Implemented Attack Surface Reductions

QTS has proactively addressed these exposures through firmware updates that introduce configurable disable options via the microSD card. These changes require no hardware modifications and maintain full backward compatibility for users who need the services.

Key Hardening Features (as implemented by QTS):

- **SSH and Web Ports Disable Option** Available in **Kernel AN-X4-KERNEL-PROD.v4.05.01.qtk** or later. By removing and/or modifying a specific file on the microSD card,



both SSH (TCP 22) and the web server (TCP 80) can be fully disabled. This eliminates remote management interfaces when local/physical configuration via card is sufficient.

- **Modbus TCP Port Disable Option** Available in **AN-X4-AB-DHP.v4.17.01.qtf or later**. Operators can now disable the Modbus TCP server (TCP 502) via a microSD card configuration change. This is ideal for deployments that do not require Modbus TCP access to DH+ stations.
- **Proprietary RIO Configuration Port Disable Option** Available in **AN-X4-ABRIO-SCAN.v4.04.01.qtf** and **AN-X4-ABRIO-ADPT.v4.05.01.qtf or later**. The TCP 42889 port (used by RIO configuration tools) can now be disabled via microSD card modification, reducing exposure in RIO scanner/adaptor deployments.

These options represent a major security improvement, shifting from “always-on” services to “explicitly enabled only when required.”

4. Conditional and Remaining Exposures

Even after applying the above reductions, some exposure may remain depending on application needs:

- **Allen-Bradley CSP (TCP 2222)**: This port is exposed **only** when Data Highway Plus HMI IP Aliases are configured. CSP support is necessary for certain legacy HMI, SCADA, or programming software (e.g., older PanelViews or RSLinx Classic). **Recommendation**: Do **not** configure HMI IP Aliases unless CSP is explicitly required. If CSP is not needed, this port remains closed.
- **Core Industrial Protocols** (EtherNet/IP, etc.): TCP/UDP 44818 and UDP 2222 (scheduled I/O) are required for the gateway's primary function and cannot be disabled. These should be strictly firewalled and segmented.

5. Configuration Steps for Maximum Hardening

1. Update to the latest compatible firmware/kernel (Kernel v4.05.01.qtk+, DHP v4.17.01.qtf+, RIO Scanner v4.04.01+ and RIO Adapter v4.05.01+).
2. Power down the module and remove the microSD card.
3. Apply the documented file removal/modification for desired disables (SSH/web, Modbus TCP, RIO config port 42889).
4. For CSP: Avoid creating entries in the HMI IP Aliases configuration file (Dhp\AnxDhpCfgHmiAlias.txt) unless required.
5. Re-insert card, power on, and verify via local diagnostics or network scan that disabled ports are closed.
6. Reboot after changes.



6. Recommended Deployment Best Practices

- **Network Segmentation:** Place the gateway in a Level 1.5 or Level 2 zone (per Purdue Model) behind a stateful firewall with strict allow-listing for only required IPs and ports.
- **Least Privilege:** Disable every non-essential service using the new microSD options.
- **Firmware Management:** Always use the latest QTS/ProSoft firmware; validate checksums and use the web interface (only when enabled) for updates.
- **Physical Security:** Restrict physical access to the module and microSD card slot.
- **Monitoring & Logging:** Enable AN-X diagnostic logs; monitor for unexpected connection attempts on any remaining ports.
- **Change Management:** Document all microSD modifications and test in a lab environment before production deployment.

7. Residual Risk Assessment

With all applicable disables applied and CSP/HMI aliases avoided:

- **Low** residual network attack surface for management services.
- Primary remaining vectors are legitimate industrial protocol traffic (EtherNet/IP, CSP if required), which must be protected by network controls.
- Overall risk profile is now consistent with modern hardened OT gateways.

Conclusion

The security enhancements introduced by Quest Technical Solutions for the AN-X4-AB-DHRIO gateway demonstrate a strong commitment to reducing the attack surface in industrial environments. By providing simple, microSD-based options to disable SSH, web, Modbus TCP, and the RIO configuration port (42889), along with clear guidance on conditional CSP exposure, QTS has transformed a previously open device into one that can be securely deployed in critical infrastructure.

Customers are strongly encouraged to upgrade to the specified firmware versions and apply the hardening steps outlined above. These measures, combined with proper network architecture, significantly improve the security posture of legacy DH+/RIO modernization projects.



NMAP Reports

AN-X4-AB-DHP – Before Mitigation

```
nmap -sT -p- 10.10.0.111
Starting Nmap 7.92 ( https://nmap.org ) at 2026-04-16 17:23 EDT
Nmap scan report for Anx4b.lan (10.10.0.111)
Host is up (0.0013s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
502/tcp    open  mbap
44818/tcp open  EtherNetIP-2
```

Nmap done: 1 IP address (1 host up) scanned in 4.98 seconds

AN-X4-AB-DHP – After Mitigation

```
nmap -sT -p- 10.10.0.111
Starting Nmap 7.92 ( https://nmap.org ) at 2026-04-16 17:30 EDT
Nmap scan report for Anx4b.lan (10.10.0.111)
Host is up (0.063s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT      STATE SERVICE
44818/tcp open  EtherNetIP-2
```

Nmap done: 1 IP address (1 host up) scanned in 3.93 seconds

AN-X4-ABRIO-SCAN – Before Mitigation

```
nmap -sT -p- 10.10.0.111
Starting Nmap 7.92 ( https://nmap.org ) at 2026-04-16 17:38 EDT
Nmap scan report for Anx4b.lan (10.10.0.111)
Host is up (0.0011s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
42889/tcp open  unknown
44818/tcp open  EtherNetIP-2
```

Nmap done: 1 IP address (1 host up) scanned in 4.03 seconds

AN-X4-ABRIO-SCAN – After Mitigation

```
nmap -sT -p- 10.10.0.111
Starting Nmap 7.92 ( https://nmap.org ) at 2026-04-16 17:44 EDT
Nmap scan report for Anx4b.lan (10.10.0.111)
Host is up (0.00036s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT      STATE SERVICE
44818/tcp open  EtherNetIP-2
```

Nmap done: 1 IP address (1 host up) scanned in 3.97 seconds



AN-X4-ABRIO-ADPT – Before Mitigation

```
nmap -sT -p- 10.10.0.111
Starting Nmap 7.92 ( https://nmap.org ) at 2026-04-16 17:52 EDT
Nmap scan report for Anx4b.lan (10.10.0.111)
Host is up (0.0011s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
42889/tcp open  unknown
44818/tcp open  EtherNetIP-2
```

Nmap done: 1 IP address (1 host up) scanned in 4.54 seconds

AN-X4-ABRIO-SCAN – After Mitigation

```
nmap -sT -p- 10.10.0.111
Starting Nmap 7.92 ( https://nmap.org ) at 2026-04-16 17:44 EDT
Nmap scan report for Anx4b.lan (10.10.0.111)
Host is up (0.00036s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT      STATE SERVICE
44818/tcp open  EtherNetIP-2
```

Nmap done: 1 IP address (1 host up) scanned in 3.94 seconds