Middle Atlantic Premium+ PDU with RackLink™ Network Security

# Middle Atlantic's Product Development Process Continually Tests and Protects Firmware Updates against Vulnerabilities

As organizational networks evolve to support higher bandwidths and new architectures, Middle Atlantic helps maximize power investments with its Premium+ power distribution units (PDUs) featuring RackLink™ technology. Premium+ PDUs with RackLink™ deliver a comprehensive suite of control, data, and security capabilities leveraging the XERUS™ platform by Raritan, the industry leader in intelligent data center power products and a sister company within the Legrand portfolio. Firmware security is a driving concern for Middle Atlantic. As Premium+ is considered a networked solution, a stringent and thorough development process is adhered to, with constant testing for vulnerabilities.

## Firmware Release Process

Firmware updates are a great way to regularly introduce customers to new features and benefits. However, updates can expose organizations to many vulnerabilities if the development process is not firmly centered around continuous monitoring and threat assessment. The update process for Middle Atlantic's Premium+ PDU with RackLink™ is designed with security at the forefront to protect users' networks and data, providing peace of mind when connecting to the network.

## Raritan: A Trusted Partner

An internal Security Working Group has been created and works in collaboration with sister company Raritan — the most trusted provider of intelligent rack PDUs for data centers in 9 of the top 10 Fortune 500 technology companies. This group is dedicated to staying ahead of the security requirements for networked power distribution units, overseeing threat assessment throughout planning and development as well as ensuring exhaustive system testing for firmware releases.

Raritan continuously monitors Common Vulnerabilities and Exposures (CVEs) and other exploits prior to and during the development process to build the most secure products possible. At the center of this process is the Nessus Vulnerability Scanner by Tenable®. Nessus is trusted by more than 30,000 organizations worldwide, making it one of the most widely deployed security technologies. Essentially, this scanner is the gold standard for vulnerability assessment.  Before a new PDU firmware gets released, it undergoes thorough testing with this scanner.

Nessus scan reports for Premium+ PDU with RackLink™ firmware releases are available upon request.

## Security Assessment Process

There are two parts to Middle Atlantic's security assessment: during planning and development and final system testing.

### During Planning and Development:

- Publicly known vulnerabilities are reviewed.
- Security issues are reviewed, evaluated, and addressed if applicable.
- An immediate Limited Availability (LA) release is created to address the severe issues, otherwise patches are deployed in the next available General Availability (GA) release.

### During System Testing:

- Each firmware release undergoes a rigorous system testing process, including security components.
- Nessus Vulnerability Scanner is used as a high-level security scanning tool to test and confirm the strength of security features.

## Nessus Testing Core

The Nessus testing procedure is designed to be a proactive approach to any arising cyber risks:

- Nessus scans are run against the XERUS™ platform controller after installing the firmware build under test and resetting to factory defaults.
- Plugins = security test cases (all available tests are used).
- Nessus decides relevance based on services running, etc.

An intense schedule of scans also helps stay ahead of any vulnerabilities. Scans are done:

- Systematically during development: 3-5 times per GA release cycle and 1-2 time for LA release cycle.
- Several weeks before a release target date to allow time for fixes.
- Always against final GA/LA builds.

Finally, scan reports are gathered and analyzed:

- Tasks are created in a development planning/tracking tool and preloaded for every release to track scans and reporting.
- Each Nessus scan generates a report, which is uploaded into the system and associated to the right release.
- This is repeated as necessary if vulnerabilities are identified and then subsequently fixed.

Middle Atlantic created its first networked PDU in 2011. The 2019 launch of Premium+ introduced the most robust security firmware features in any PDU for AV systems. These vulnerability assessments and management processes are at the core of providing a fully updated, solid, and secure solution. Middle Atlantic's Premium+ PDU with RackLink™ products are designed to be as secure on the inside as they are powerful on the outside.