Security Vulnerability Policy

Overview

A+ Technology & Security follows industry best practices in managing and responding to security vulnerabilities in our products in order to minimize customer exposure to cyber risks. There is no way to guarantee that products and services are free from flaws that can be exploited for malicious attacks. This is not specific to A+ Technology & Security, but rather a general condition for all network devices. What A+ Technology & Security can guarantee, is that we always make a concerted effort at every possible stage in order to ensure that the least risk possible is associated with your A+ Technology & Security devices and services.

A+ Technology & Security acknowledges that standardized network protocols and services may have weaknesses that may be exploited for attacks. While A+ Technology & Security cannot take responsibility for these services, we are dedicated to providing recommendations on how to reduce and eliminate risks relating to your A+ Technology & Security devices.

The latest applicable security patches are included in the latest software/firmware releases. A+ Technology & Security provides free software and firmware updates for products covered under our Software Upgrade Protection Program. These updates can be downloaded by visiting the documents download section of each product's page on our website: www.aplustechnology.com.

Vulnerability Management

A+ Technology & Security classifies the severity of a vulnerability as either critical or non-critical. The classification is based on the risk for users when products are deployed, hardened and used in a recommended way. Newly discovered vulnerabilities that A+ Technology & Security classifies as non-critical will be managed in the normal scheduled firmware release cycle.

Newly discovered vulnerabilities that A+ Technology & Security classifies as critical may result in an unscheduled service release for applicable and supported firmware. A security advisory will be published at www.aplustechnology.com/product-security including a case description, threat/risk analysis, recommendations and A+ Technology & Security's plan to resolve the issue.

Reporting Vulnerabilities

While A+ Technology & Security will work to limit risks associated with vulnerabilities, if you identify a security vulnerability associated with an A+ Technology & Security product or service, please report the problem immediately. Timely identification of security vulnerabilities is critical to eliminating potential threats.

End users, partners, vendors, industry groups and independent researchers who have identified a potential risk are encouraged to email product-security@aplustechnology.com. Please check www.aplustechnology.com/product-security before contacting the team as your concern may already have been processed in a security advisory.

Note: A+ Technology & Security's product security team will not process requests for support, modified features and statements. Such requests need to be sent through the appropriate A+ Technology & Security channel, typically sales or technical support.

Technical support: www.aplustechnology.com/support
General: www.aplustechnology.com

Response Process

All valid submissions to product-security@aplustechnology.com will be processed and analyzed. A+ Technology & Security will reply within 48 hours with an acknowledgement and possible additional questions for investigation. Depending on severity level, A+ Technology & Security may follow up by posting further information on www.aplustechnology.com/product-security.

Receiving Information from A+ Technology & Security

A+ Technology & Security publishes guidelines, security advisories and statements on www.aplustechnology.com/product-security.

*Please note that the advice and suggestions contained in this flyer are provided for informational purposes only and should not be construed or relied upon as comprehensive or exhaustive advice on how to protect your systems from cyber vulnerabilities. A+ Technology & Security does not guarantee that any of its products are immune from a potential cyber-attack and adhering to the advice and suggestions contained in this flyer may still result in your system being subject to cyber vulnerabilities or a cyber-attack.

A+ TECHNOLOGY & SECURITY

631.969.2600
info@aplustechnology.com

1490 North Clinton Ave.
Bay Shore, NY 11706