

## **Aruba Security Incident Response Policy**

### **1.0 Introduction**

Aruba Networks actively works with industry security organizations and Federal security governance bodies responsible for security incident response guidelines to provide both pro-active and reactive support when security vulnerabilities are reported. Aruba is committed to developing its hardware and software products so as to ensure any reported vulnerabilities are mitigated appropriately. Aruba Networks provides customers, outside agencies, and other security response groups with the ability to report any security related vulnerabilities through our WSIRT (Wireless Security Incident Response Team). Identifying potentially threatening vulnerabilities is an important step in protecting customer network infrastructures and information contained within the systems managed by these networks.

### **2.0 Reporting Suspected Security Vulnerabilities**

Aruba Networks provides several methods and tools by which potential security vulnerabilities can be reported to Aruba's WSIRT. Aruba's WSIRT is available 24X7 to work with customers and reporting agencies to receive potential vulnerabilities in order to evaluate impacts to Aruba products and software, and assign classification of threat level. The main way to reach these reporting mechanisms is through the Aruba Networks WSIRT web site located at <http://www.arubanetworks.com/support/wsirt.php>.

Email notification to Aruba's WSIRT is the preferred method of reporting vulnerabilities because any information reported needs to be treated as confidential and can be encrypted using our PGP key. However, if you are uncertain as to whether you are experiencing a vulnerability, your first contact should be to the Aruba Technical Assistance Center (TAC). Our technical support professionals will work with you to determine if your issue is related to a potential vulnerability, or an issue related to configuration or product defect unrelated to vulnerability.

#### ***2.1 Contacting Aruba TAC***

. If you are experiencing a network outage related to a security incident, or are having problems configuring a security feature, please contact Aruba TAC at 1 (800) WiFiLan (1-800-943-4526) / International: 1-408-754-1200.

## ***2.2 Reporting to Aruba WSIRT***

If a security problem or vulnerability is found in an Aruba product, please send us an email with detailed description of the problem. Once we acknowledge your email, we request five business days to reproduce the reported problem and prepare a response. We appreciate you waiting for our response prior to reporting the problem to others.

When reporting, please try to include the following:

1. High-level description of the problem along with a technical contact we can get in touch with who can answer all related questions.
2. List of Aruba hardware involved
3. List of Aruba software versions involved
4. A detailed description of the issue which ideally provides enough information to reproduce the problem
5. Logs and other supporting information

Email sent to [wsirt@arubanetworks.com](mailto:wsirt@arubanetworks.com) is distributed to a select group of Aruba employees who are experienced in handling security related issues. Please use the PGP keys found at: <http://www.arubanetworks.com/support/wsirt.php> for encrypting any sensitive information sent to the WSIRT.

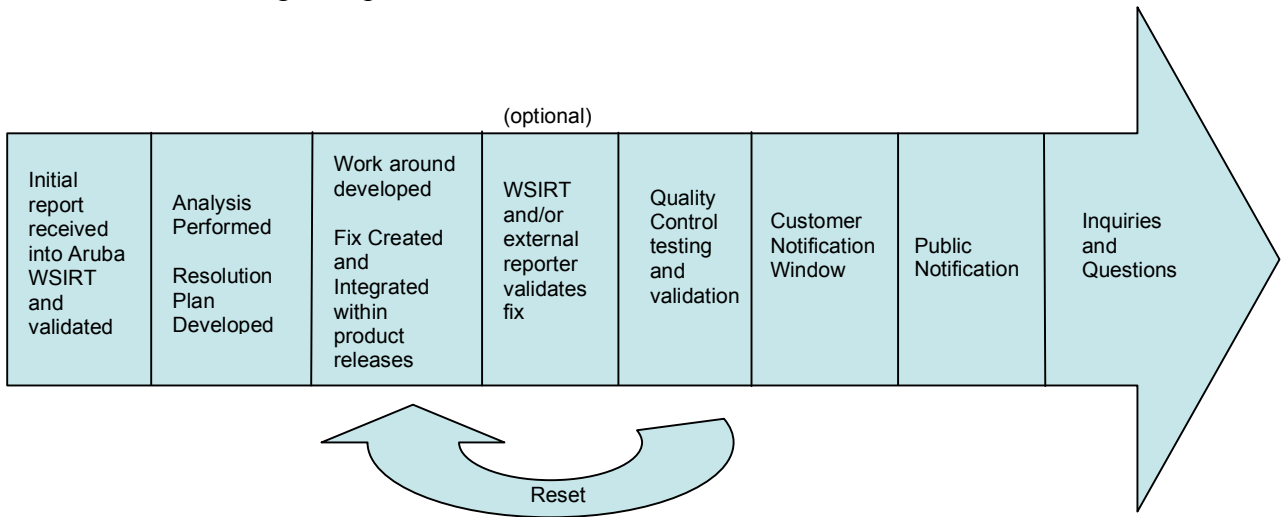
## **3.0 Aruba Security Vulnerability Response Process**

All reports sent to the Aruba WSIRT concerning suspected or potential existence of a vulnerability related to Aruba products are reviewed and processed by Aruba's WSIRT. This review is performed utilizing the written description of the suspected vulnerability and any data collected by the reporter. Each report is evaluated against criteria designed to determine whether or not the report is a qualified vulnerability. In some cases it is necessary to request additional information from the reporting entity in order to begin the review.

Aruba WSIRT utilizes a thorough review and analysis process designed to provide the best qualification and categorization of reported vulnerabilities. We require detailed technical information and scenario-based descriptions from the reporter in order to ensure a successful evaluation can be completed. After the Aruba WSIRT, in conjunction with the Aruba ATL (Aruba Threat Lab), performs initial evaluation, assignment of severity level is made. The WSIRT will contact the reporter in order to update the status of the

investigation and the severity level of the vulnerability should one exist. WSIRT will work with the reporter to negotiate the planned timeframes for resolution, as well as the customer and public communication plans.

The following process flow demonstrates the components of Aruba’s vulnerability assessment and mitigation process:



Note: The length of time for this process will depend on the severity level of the validated vulnerability

Aruba’s WSIRT has overall responsibility for managing the process of development and distribution of workarounds and patch releases for the vulnerability. This oversight is required to ensure that during the notification process, the appropriate aspects of customer support are met. Once the workarounds and patch releases are ready for customer distribution, WSIRT is responsible for making them available on the WSIRT web site for easy access by customers.

All information received by the Aruba WSIRT is considered confidential, and as such is restricted to a limited group of Aruba subject matter experts with specific skills designed to provide the most comprehensive resolution action plan. In addition, the WSIRT will ask the reporter to treat the information as confidential until such a time as Aruba can provide customers with resolution plans and options for mitigation through the WSIRT web site located at: [www.arubanetworks.com/support/wsirt.php](http://www.arubanetworks.com/support/wsirt.php) , as well as a coordinated customer and public disclosure.

#### **4.0 Disclosure policy**

Reports of potential vulnerabilities are treated as confidential within the Aruba WSIRT. All work within Aruba concerning resolution of vulnerabilities is done within a restricted set of team members who understand the importance of confidentiality with regard to aspects of security vulnerability investigations. Aruba works with vulnerability reporting entities to keep confidential the information related to the vulnerabilities. Keeping information relating to the vulnerability confidential is critical, from the time of reporting through the time of public notification.

When the necessary patches and workarounds are developed and available, customers will be notified. The customer notification window will be 30 days before public disclosure. It is Aruba's policy to notify all of its customers of vulnerabilities at the same time. Disclosure is not selective under any circumstances, other than when there exists a potential impact to national security.

#### **5.0 Security Advisories**

Security advisories are published on the Aruba Networks WSIRT web site: [www.arubanetworks.com/support/wsirt.php](http://www.arubanetworks.com/support/wsirt.php). This site is where you will find the latest advisory, as well as an archive of previous advisories.

Advisory notices are sent at the same time via email to all customers registered with the Aruba Support Center. Should you wish to receive these advisory notices, please register with the Support Center at: <https://support.arubanetworks.com/login.php>.

Advisory alerts are also announced on Aruba Networks Support Center web site: <https://support.arubanetworks.com/login.php>.