aruba
a Hewlett Packard Enterprise company

ARUBA SECURITY INCIDENT RESPONSE POLICY

INTRODUCTION

Aruba actively works with industry and government security organizations responsible for security incident response guidelines to provide proactive and reactive support when security vulnerabilities are reported. Aruba is committed to developing its hardware and software products to ensure any reported vulnerabilities are mitigated appropriately. Aruba provides customers, outside agencies, and other security response groups with the ability to report any security related vulnerabilities through the Aruba SIRT (Security Incident Response Team). Identifying potentially threatening vulnerabilities is an important step in protecting customer networks and information contained within the systems managed by these networks.

REPORTING SUSPECTED SECURITY VULNERABILITIES

Aruba provides several methods and tools by which potential security vulnerabilities can be reported to Aruba's SIRT. The SIRT 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 SIRT web site located at http://www.arubanetworks.com/support-services/security-bulletins.

Email notification to Aruba's SIRT is the preferred method of reporting vulnerabilities. Any information reported should be treated as confidential and should be encrypted using PGP keys or S/MIME. 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). Aruba 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.

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 using the options found at http://www.arubanetworks.com/support-services/support-program/contact-support/.

Reporting to Aruba SIRT

If a security issue 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 sirt@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-services/security-bulletins for encrypting any sensitive information sent to the SIRT.

ARUBA SECURITY VULNERABILITY RESPONSE PROCESS

All reports sent to the Aruba SIRT concerning suspected or potential existence of a vulnerability related to Aruba products are reviewed and processed by Aruba's SIRT members. 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 SIRT 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 SIRT performs an initial evaluation, assignment of severity level is made. The SIRT will contact the reporter in order to update the status of the investigation and the severity level of the vulnerability should one exist. Aruba SIRT will work with the reporter to negotiate the planned timeframes for resolution, as well as the customer and public communication plans.

Aruba's SIRT 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, the Aruba SIRT will publish advisories on the SIRT web site for easy access by customers.

All information received by the Aruba SIRT 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 SIRT 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, as well as a coordinated customer and public disclosure. Where the reporter wishes to receive public acknowledgement or "credit" for finding the vulnerability, Aruba will provide that in the published security advisory.

DISCLOSURE POLICY

Reports of potential vulnerabilities are treated as confidential within the Aruba SIRT. 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 initial notification will consist of general information about the vulnerability, workarounds, and steps to eliminate the vulnerability. After 60 days, Aruba will update the published advisory to provide "full disclosure" – the hope is that through sharing of information, the overall state of the information security industry can be improved.

It is Aruba's policy to notify all customers of vulnerabilities at the same time. Disclosure is not selective under any circumstances – no Aruba customer is given advance notification of a vulnerability. Aruba's OEM partners are generally notified three days in advance of public disclosure to allow their respective security response teams to prepare for notification of their own customers. Aruba's OEM partners have agreed contractually to coordinate vulnerability notifications with Aruba so that all end users are alerted at the same time.

SECURITY ADVISORIES

Security advisories are published on the Aruba Networks WSIRT web site: http://www.arubanetworks.com/support-services/security-bulletins/. This site is where you will find the latest advisories, 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.

Advisory alerts are also announced on Aruba's Support Center web site under the Announcements tab: https://support.arubanetworks.com.

GT_SecurityIncidentPolicy_030419