Avaya's Product Security Vulnerability Response Policy

Abstract

Avaya's goal is to deliver secure, reliable products. However, Avaya recognizes that in today's environment, security vulnerabilities may be identified after a product is launched. These vulnerabilities may occur in Avaya developed capabilities, embedded technologies, and in execution environments on which Avaya products operate. In each of these cases, Avaya looks to active threat monitoring, rapid assessment and threat prioritization, response and proactive customer contact, and expedited remediation, to help resolve security vulnerabilities.

This document describes Avaya's Product Security Vulnerability Response Policy ("Policy"). This Policy does not apply to all Avaya products. Some products may be covered by other Avaya policies and procedures. Avaya does not guarantee that all security vulnerabilities will be detected and/or remediated.

Table of Contents

1. INTRODUCTION 3
2. MONITORING 3
3. ASSESSMENT 4
4. NOTIFICATION 4
5. REMEDIATION 5
6. REPORTING A SUSPECTED SECURITY VULNERABILITY 7

1. Introduction

In order to respond to security vulnerabilities, Avaya has created a Vulnerability Threat Management (VTM) system. This Policy will be used as guidance for tracking, categorizing and responding to security vulnerabilities.

This Policy describes the sources which are tracked and the Avaya security response process. This Policy supersedes all previous policy or practice documents regarding this topic for the products covered by this Policy.

The overall VTM process is divided into four stages: Monitoring, Assessment, Notification, and Remediation. These stages are explained in the following sections.

2. Monitoring

During the monitoring stage, Avaya will actively monitor security notification sources. Avaya has chosen to monitor information provided by only those sources which generally meet the following criterion:

- A vendor of a product which is incorporated in Avaya products
- A government agency which is vendor-agnostic and is deemed by Avaya to be reputable in their information

Although numerous sources may be monitored for information Avaya will generally rely on the below sources, as updated from time to time by Avaya, to trigger the Avaya VTM process and the creation of an Avaya Security Advisory.

- Apache Tomcat
- CentOS
- Hewlett Packard
- Microsoft
- Oracle
- PostgreSQL
- Red Hat
- US-CERT
- VMware
- Wind River
- IBM
- Apple
- Xen

Avaya also may issue advisories based on information obtained outside of these sources. This may include customer or third party findings, internal development, or research efforts.

3. Assessment

Once a security notification from a monitored source is received, the applicability of the reported issues to Avaya products will be determined. Avaya uses the Common Vulnerability Scoring System version 3 ("CVSSv3") as a part of our process for evaluating potential vulnerabilities in Avaya products. As a standard part of our assessment we will obtain the CVSSv3 base score as reported by the National Institute of Standards and Technology in the National Vulnerability Database or the vendor for the affected component. In some cases, such as where a CVSSv3 base score is not available from NIST or the vendor, Avaya will calculate the CVSSv3 base score. The overall severity of that security notification will be determined by the highest CVSSv3 base score calculated for any single vulnerability in the security notification and assigned one of five severity classifications:

CVSSv3 Base Score	Severity Classification
9.0 – 10.0	Critical
7.0 – 8.9	High
4.0 – 6.9	Medium
0.1 – 3.9	Low
0.0	None

More information on CVSS and how the score is calculated can be obtained from https://www.first.org/cvss/.

4. Notification

Once the assessment phase has produced an initial rating customers are notified of the applicability and classification of the reported vulnerabilities through the creation of an Avaya Security Advisory ("Advisory").

The Advisory is posted on the Avaya Support Website https://support.avaya.com/security and notification of the posting is made through a bulk email distribution for those who have signed up to receive notification on the Avaya Support Website.

Based on the nature of the vulnerability and its classification, the Advisory may include a recommended mitigation action, a recommendation regarding the use of a 3rd party provided patch, a planned Avaya software patch or upgrade, and/or additional guidance regarding the vulnerability. The suitability of following or using any recommendation, guidance, patch or upgrade shall be made solely by the customer.

Depending on the classification, Avaya will attempt to provide notification based on the following time targets:

Severity Classification of Vulnerability	Target Intervals for Assessment and Notification from Avaya
Critical	Within 1 business day
High	Within 3 business days
Medium	Within 1 week
Low	Within 2 weeks
None	At Avaya's discretion

Avaya will use reasonable efforts to make an initial assessment within these targets after notification from an advisory group.

To receive proactive notification of new and updated Advisories, users can register with the Avaya E-Notification Services by performing the following steps:

1) Browse to https://support.avaya.com
2) If an account hasn't been created, select "Register Now" and create an account.
3) Enter the account credentials and select "Login".
4) Once logged in, click on the "Set E-notifications" link at the bottom of the page.
5) This opens up the "E-Notifications" page with all the available notifications.
6) To receive notification for all Advisories as they are posted, in the general notifications list click the check box next to "Security Advisories" and click on "Update". If the check box is already checked then no further action is required.
7) To receive notifications for an individual product and release, click on "Add More Products" in the product notifications section. Scroll down the list and select the product, select the release of the product from the "Select a Release Version" drop-down selection box, select the box for "Security Advisories" and click on the "Submit" button. Repeat for additional products.
8) When finished adding products, select "My Notifications" to return to the main E-Notifications page. All products added from the previous steps should be listed in the product notification section.

The client is now ready to receive email E-Notifications whenever a new Advisory is published or an existing Advisory is updated.

5. Remediation

When a notification is issued by Avaya in the form of an Advisory, mitigation and/or remediation actions may be included in the notification.
When a 3rd party patch is available to mitigate a vulnerability, Avaya may recommend the patch from the 3rd party be applied by the customer. This action, if recommended, will be explicitly stated in the Advisory.

For some 3rd party patches, Avaya may not recommend installation due to interoperability, stability or reliability issues with the patch and the Avaya product. Customers who apply 3rd party provided patches without Avaya's recommendation may void their warranty.

In some instances, when a software vendor provides a patch to address a vulnerability, Avaya may determine to address the vulnerability through other means to avoid potential risks to Avaya applications. This may include the modification of existing software through an Avaya-issued patch that is released separately or incorporated into future releases of the product. Such decision to offer an alternative remediation will be described in the Advisory.

Based on the severity classification and the availability of a vendor supplied patch, Avaya will use reasonable efforts to provide remediation actions based on the following target intervals:

NOTE: Avaya is dependent on many factors to meet the target remediation action intervals (defined in the previous table), including vendors providing updated components in a timely manner. These timeframes are targets and not guarantees.

Severity Classification of Vulnerability	Target Intervals for Remediation Action
Critical	If a software patch needs to be developed by Avaya it will be released as a patch, service pack, or update as soon as reasonably possible. If a software patch or other mitigation is available, recommended actions will be described in the Advisory.
High	If a software patch needs to be developed by Avaya, it will be included in the next service pack or update where the patch can be reasonably incorporated. If a software patch or other mitigation is available, recommended actions will be described in the Advisory.
Medium	If a software patch needs to be developed by Avaya, it will be included in the next minor release where the patch can reasonably be incorporated. If no new minor releases are scheduled for a product, and Avaya is providing maintenance support, Avaya will incorporate the fix into a service pack or update. If a software patch or other mitigation is available, recommended actions will be described in the Advisory.

Low	If a software patch needs to be developed by Avaya, it will be included in the next major or minor release where the patch can reasonably be incorporated. If no new major or minor releases are scheduled for a product, and Avaya is providing maintenance support, Avaya will make reasonable efforts to incorporate the fix into a service pack or update. If a software patch or other mitigation is available, recommended actions will be described in the Advisory.
None	No remediation actions will be required.

6. Reporting a Suspected Security Vulnerability

6.1. For Avaya Customers and Business Partners:

While Avaya is committed to helping our customers operate their Avaya systems and networks securely, the customer is responsible for the security of their environment. Customers with information regarding any suspected security problems with Avaya products can create a Service Request through their normal support channel by either using the Self Service link on the Avaya Support Website, or contacting the Customer Support phone number under the Maintenance Support Link (1-800-242-2121 for US domestic customers).

6.2. For external security researchers:

Security researchers who are not Avaya customers or business partners wishing to report a suspected security finding with Avaya products can email securityalerts@avaya.com.