AVAYA communication

Security Vulnerability Escalation

Prerequisites

Issue 1.1
November 7, 2018

DISCLAIMER

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. Avaya does not guarantee that all security vulnerabilities will be detected and/or remediated.

THE INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. USERS ARE RESPONSIBLE FOR THEIR APPLICATION OF ANY PRODUCTS COVERED BY THIS DOCUMENT. THIS DOCUMENT IS INTENDED TO PROVIDE GENERAL INFORMATION AND IS NOT MADE PART OF ANY AGREEMENT YOU HAVE WITH AVAYA RELATED TO YOUR PURCHASING AND/OR LICENSING OF AVAYA PRODUCTS AND RELATED WARRANTY, MAINTENANCE AND SUPPORT. AVAYA INC. MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY THREATS TO CUSTOMERS' SYSTEMS. YOUR RESULTS MAY VARY DEPENDING ON, AMONG OTHER THINGS, THE SECURITY CONFIGURATION OF YOUR NETWORK. THE INFORMATION PROVIDED IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE.

Due to the inherent knowledge needed to properly configure systems and networks to comply with the customer's policies, the customer ultimately is responsible for the appropriate security configurations on their data network and systems including additional OS hardening, where applicable.

Contents

Introduction

The purpose of this document is to provide guidance to Avaya customers regarding Avaya's process for handling customer-identified security vulnerabilities. This includes providing guidance on how to manage mapping necessary components to identify a suspected vulnerability and the action(s) a customer may take to mitigate/correct the vulnerability. It also describes next steps a customer may take if no appropriate action(s) exists and provides the necessary steps to take to engage Avaya. This document supports the *Product Security Vulnerability Response Policy*, *Avaya's Security Vulnerability Classification*, and *Avaya Product Lifecycle Policy* documents.

These documents and all information related to identified Avaya product vulnerabilities can be found at http://support.avaya.com/security. Click on Product Notices > Security Advisories for a list of advisories by product. Avaya Security Advisories (ASAs) are now also cataloged by year or are searchable based on product release. To search for ASAs based on product/release, start at https://support.avaya.com > Support by Product > Documents. Select target product/release, and then select "Security Advisories." You may also view the PCN and PSN report summary by clicking here.

Avaya takes vulnerability handling seriously and has programs in place to help you address potential vulnerabilities appropriately.

Mapping CVEs to ASAs

When a vulnerability analysis application is directed towards an Avaya system, the resulting data typically includes a list of commonly known vulnerabilities that could potentially impact the target system. These results are eventually reviewed by security experts with specific configuration knowledge of the system to determine their validity, and help rule out false positives.

Through the monitoring of vendor security alert mailing lists, Avaya creates Security Advisories which detail the products/releases impacted by the vulnerabilities called out by these vulnerability analysis applications. By mapping a particular vulnerability to an Avaya Security Advisory (ASA), one can deduce which Avaya products may be affected by that vulnerability.

Purpose

This document section outlines a means of searching and mapping known Common Vulnerability Exposure (CVE) numbers and security alerts from vendors (e.g. Red Hat, Microsoft) to associated Avaya Security Advisories. It is intended for Avaya support engineers as well as business partners and end customers, and provides different methods anyone can use to help confirm whether a known vulnerability impacts a particular product/release. These methods require knowledge of common Web searching tools, and in some cases, they may require shell access to the products themselves.

Standard Web Searching

Since ASA and CVE numbers are publicly available data, a common Web-based search tool may be used. Performing a search on a common search site for *"Avaya CVE-2015-5364"* will very likely return a reference to https://support.avaya.com in the top list of results. This link is a direct link to an Avaya Security Advisory which covers the searched CVE. This link can be followed to determine which of Avaya's products may be affected, as well as what Avaya has provided for guidance to mitigate or resolve the issue. Sometimes a single CVE can map to multiple ASAs, in which case the search site should find all related ASAs.

Avaya Support Site

An alternative to using a standard Web-based search mechanism is to go directly to https://support.avaya.com/security. Once on this site, in the search box on the upper right hand corner of the page, enter the CVE number or Security Alert ID (e.g., RHSA-2015-1623) to search for surrounded in quotes. Links to any associated ASAs should show up as results.

When No ASA is Found

If a CVE number cannot be mapped to an Avaya Security Advisory, reasons could include:

- If the CVE has been recently created, it is possible that the operating system vendor does not yet have a security alert for the vulnerability. If this is the case, Avaya will publish an Avaya Security Advisory soon after the alert is published by the vendor. Avaya has the Product Security Vulnerability Response Policy that outlines timeframes for publishing Avaya Security Advisories:

- There are also cases where the vendor may not have a security alert for a particular vulnerability. To determine this, follow a search result link pointing directly to the CVE number itself, commonly on http://cve.mitre.org.

  Key word searches may also help in cases where there is no CVE.

For software only applications, the OS should regularly be updated as defined by the OS vendor, and allowed in the appropriate Avaya software requirements section for that Avaya tool or product. The tool or product manuals on support.avaya.com may document any known dependencies on required software installed on the server. One may follow the software application's tools or product software requirements, staying within that tool or product's documented guidance.

Performing Manual Package Version Lookups

If an Avaya Security Advisory is not found, or it is unclear if a specific release of a product may be affected, the best way to determine if a product may be affected by a known vulnerability is by manually looking up the version of the package installed on the product. This is most ideal when dealing with products running on a distribution of Linux. If a corresponding Red Hat Security Alert (RHSA) can be identified as covering a particular vulnerability, the RHSA contains the package version(s) containing the resolution to the issue(s). If possible, compare the listed package version(s) outlined by the RHSA with the version of the package or packages installed on the Avaya product in question. This manual comparison should be enough to determine if the Avaya product is still vulnerable or not.

NOTE: Package version lookups require shell access to the system as well as knowledge of the *rpm* "query" Linux command ("rpm –q <package_name>").

Searching Avaya-Modified Packages

For some products, such as Communication Manager, various packages have been modified from the original vendor distribution. In these cases, the package name of an installed package will contain the extension "AV". When performing manual package version lookups for security updates, it is possible that one may come across a package with an "AV" extension. In most cases, the base version of the package itself should be used when determining what security fixes are in the package. If a case arises where a security update is not included in the base version of a package with an "AV" extension, the change log of the package may be viewed to determine if Avaya has added a security patch to the package. To check the change log of a package, run the command:

```
rpm –q --changelog <package_name>
```

If any vulnerability fixes have been included in the modified package, a note about the fix might be found in the change log.

When These Search Methods Aren't Enough

If any of these search methods do not help in determining if a product contains a security update, create a Service Request by following this link. This link requires SSO login credentials.

Engaging Avaya

Follow these guidelines if you believe you have identified suspected software vulnerability in an Avaya product or service support tool.

Interpreting Third-Party Security Vulnerability Reports

Third-party vulnerability scanning software may be used to identify vulnerabilities. This software produces raw data that must be interpreted before contacting Avaya. Minimum information needed to research a security vulnerability:

1. Scanner software name and version
2. Type of vulnerability scan (software, compliance, HTTP/Web, etc.)
3. Finding details from scan report
4. Avaya product or application (e.g. CM, MM etc.)
5. OS name and version, and is OS provided by Avaya or customer?
6. Release and patch information for the product/application

An example of acceptable interpreted raw data format can be found in Exhibit A.

Once this raw data is interpreted, check the findings against the following available resources to see if the vulnerability has already been identified and addressed:

- Common Vulnerability Exposures (CVEs) are located at http://cve.mitre.org.

- Avaya Security Advisories (ASAs) can be found at https://support.avaya.com/security. The ASAs are categorized by product and can be searched by the related CVE or key words. These contain information about the vulnerability and any mitigating steps we recommend.

- Vulnerability Threat Management (VTM) coverage ends at end of manufacturer (EOMS) support (for software). Refer to the *Lifecycle Summary Matrix* for more details.

Alternatively, Avaya Professional Services (APS) will interpret raw vulnerability scans for a fee. Contact your Avaya account representative or Channel Partner for more information, or to purchase this service.

Reporting a New Vulnerability

If after performing the above due diligence you discover that you have potentially identified a new vulnerability:

- Open a ticket with Avaya Services if you are an Avaya customer or an Avaya Business Partner with an active maintenance agreement and create a Service Request by clicking this link.
- Login to support.avaya.com with your customer or partner SSO account
- Be sure to attach your filtered scanned file(s) when prompted.

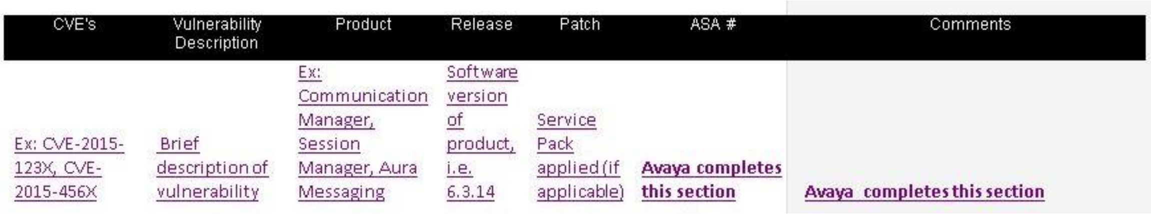
Be sure to provide all relevant details as outlined in section: Interpreting Third-Party Security Vulnerability Reports.

Protect Yourself

If you believe you're experiencing an active attack you may want to engage local law enforcement and a third-party specialist to assist in a forensic investigation.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Exhibit A



CVE's	Vulnerability Description	Product	Release	Patch	ASA #	Comments
Ex: CVE-2015-123X, CVE-2015-456X	Brief description of vulnerability	Ex: Communication Manager, Session Manager, Aura Messaging	Software version of product, i.e. 6.3.14	Service Pack applied (if applicable)	**Avaya completes this section**	**Avaya completes this section**