Avaya's Security Vulnerability Classification

Abstract

The following document defines the measurements and metrics used to qualify the level of risk an Avaya product exhibits relative to a published vulnerability. This document is used as the basis for classifying Avaya products relative to any particular vulnerability.

Table of Contents

1. Introduction

As part of the security rapid response process, the Avaya Product Security Support Team (PSST) has established an objective set of measurements which are use to determine the level of risk an Avaya product demonstrates to a particular vulnerability.

The purpose of these guidelines is to provide a consistent classification of risk level in order to assist Avaya customers in determining the seriousness of vulnerabilities outlined in Avaya Security Advisories. Based on the classification of risk determined for a product, relative to a vulnerability, different actions may be pursued and/or recommended.

2. Levels of Risk

When a product is assessed for risk to a particular vulnerability, the assessment will result in the product being categorized into one of four levels of risk. These levels of risk correspond to the priority that Avaya suggests customers associate with the vulnerability relative to the related Avaya products. The overall advisory impact will be outlined as a "Risk Level" in the Avaya Security Advisory text.

Avaya bases risk level assessments on investigation and technical analysis of the type of vulnerability and the effort required to exploit the vulnerability if left unpatched. During our technical analysis Avaya makes a conservative assumption that the vulnerability is known and that the vulnerability, if technically feasible, will be exploited.

3. Generally Accepted Secure Computing Practices

For each of the risk level categories, certain presumptions may be made regarding the ability of customers to provide mitigating controls using generally accepted secure computer practices. These include practices such as modifying access control lists, eliminating unnecessary accounts, and updating firewall policies. When these assumptions are made they will be documented in the Avaya Security Advisories text under a section entitled "Mitigating Factors".

Categorization of a product's risk may be lowered based on the ease with which a customer may be able to mitigate the risk using generally accepted secure computing practices. These mitigating actions will be documented in the Avaya Security Advisory text under a section entitled "Recommended Actions".

Defined Levels of Risk
The four levels of risk are defined as follows:

3.1. HIGH

A product's risk to a particular vulnerability is categorized as HIGH if the following criteria are met:

- An exploit can easily be performed by a remote unauthenticated attacker which provides a high-level administrative control of a system and/or a critical application AND does not require user interaction beyond standard operating procedures.

OR

- An exploit can be easily performed by a remote unauthenticated attacker which causes the system and/or a critical application to shutdown, reboot, or become unusable AND does not require user interaction.

3.2. MEDIUM

A product's risk to a particular vulnerability is categorized as MEDIUM if no higher criteria are met, but the risk does meet the following criteria:

- An exploit can be performed which provides access to a user account AND does not directly provide the privileges of a high-level administrative account.

OR

- An exploit can be performed which causes the system and/or critical application to shutdown, reboot, or become unusable AND would require existing administrative or local account access.

OR

- An exploit can be performed which allows a local user account to escalate privileges.

3.3. LOW

A product's risk to a particular vulnerability is categorized as LOW if no higher criteria are met, but the risk does meet the following criteria:

- An exploit can be performed which may be difficult or unlikely without non-standard direct user interaction but could still lead to compromise of the confidentiality, integrity, or availability of resources.

OR

- An exploit can be performed which causes non-critical applications to shutdown, reboot, or become unusable.

3.4. NONE

A product's risk to a particular vulnerability is categorized as NONE if the Avaya product is not susceptible or affected by exploitation attempts. Avaya Security Advisories rated as a risk level NONE indicate that the affected software package(s), module(s), or configuration(s) are not utilized on an Avaya product.