Upgrade Umbrella Virtual Appliance to Version 3.3.2

Contents

Introduction

This document describes how to upgrade Umbrella Virtual Appliance (VA) to version 3.3.2.

Overview

Umbrella customers running VA version 3.3.1 or earlier are recommended to upgrade their VAs to version 3.3.2.
Version 3.3.2 is a patch release that addresses a vulnerability in the key-based SSH access mechanism.

Note that an attacker can have access to the VA in order to potentially exploit this vulnerability. Unless a VA is deployed with a public IP address (which is not recommended by Cisco), the attack surface is restricted to the internal network only.

SSH-based access is not enabled for VAs running on VMware and Hyper-V by default. If you have deployed VAs on these hypervisors and have not explicitly enabled SSH access, your VAs are not subject to this vulnerability.

If your VAs on VMware, Hyper-V, KVM or Nutanix are running versions prior to 3.3.2, you can disable SSH using the command *config va ssh disable* on the VA console. This state is persisted upon VA upgrade, and you can choose to re-enable SSH access once the VA is running version 3.3.2.

SSH access cannot be disabled on VAs running on AWS, Azure and GCP. Cisco recommends setting security rules on these platforms to restrict access on port 22 of the VA only to specific VMs that are used to configure the VA. Customers running VAs on these platforms are advised to check the VA version and upgrade to version 3.3.2 if required at the earliest.

If you have not changed the default auto-upgrade settings for the VA on the Umbrella dashboard, your VAs would have auto-upgraded to version 3.3.2 by default.
For VAs that are not running version 3.3.2, you see an upgrade button against each such VA on the Sites and Active Directory page of the dashboard, which you can click to upgrade to this version.

Ensure that your VAs are able to access disthost.umbrella.com in order to be able to download the newer version.

You can also choose to redeploy your VAs if they are running very old versions - in this case, ensure that you download the latest version of the VA from the Sites and Active Directory page and use that to deploy the VA. In this case, the VA is running version 3.3.1 and auto-updates to version 3.3.2.

Cisco is not aware of any malicious use of the mentioned vulnerability.