Outpost24

Vulnerability Management made easy

HIAB Offline Enrollment and Update

Version: 1.0

2018-09-14

Table of Contents

About This Document

This document describes the encrypted communication when doing an enrollment or an update in offline mode. It lists what information is included in the different steps, what information is send in the string when enrollment is sent to Outpost24, and what is included with the returned package.

For support information, visit https://www.outpost24.com/support

1 Introduction

If the HIAB is placed in a closed network and lack contact with the OUTSCAN front end, an offline enrollment and update can still be done.

2 Offline Enrollment

***Note**: This function is only available from version 4.1.149 and onward.*

Follow these steps to enroll the HIAB without external network access.

***Note**: No customer related information is extracted from the HIAB and sent to Outpost24.*

1. The user generates an enrollment key on the HIAB that contains:
   ***Note**: The Enrollment Package is bound to the generated key, i.e. it can only be uploaded on the specific HIAB on which the key was generated. Similarly, the key is bound to the HIAB on which it was generated.*
   - Key file with random generated uuid.
     The key file is used to make sure that the enrollment package only can be installed on this HIAB.
   - Information if the HIAB is virtual or not.
   - MAC address.
   - List of installed rpm packages on the HIAB.
   - A certificate is generated on the HIAB and the public key and certificate signing request are included in the enrollment key.
2. The information is signed and encrypted and then presented to the user.
3. The enrollment key is validated on OUTSCAN to make sure that user has an active license.
4. The enrollment key is then used on OUTSCAN to generate an enrollment package containing:
   - A SQL file which updates the license information.
   - The key file with the uuid that was send in the enrollment key.
   - A file that updates vulnerability definitions.
   - A file that updates exploits information.
   - The list of installed packages send in the enrollment key are compared with available packages, any packages that should be updated/installed are included in the enrollment package.
   - A certificate is generated based on the certificate signing request and included in the enrollment package.

5. The information is signed and encrypted and the enrollment package file (enroll.pgp) is downloaded by the user.
6. The user uploads the enrollment package on the HIAB.
7. The HIAB validate that the key file in the package is the same as the one created when the enrollment key was generated.
8. The vulnerability definitions and exploits information are inserted into the database.
9. The license information is updated in the database.
10. The rpm packages are installed/updated.
11. The certificate is saved on the HIAB.
12. The HIAB is then restarted.

3 Offline Update

The offline update process is done in a similarly fashion.
Follow these steps to update the HIAB without external network access.

***Note**: No customer related information is extracted from the HIAB and sent to Outpost24.*

1. The user generates an update key on the HIAB by clicking the Generate Download Key button.

   The key contains:
   - The subject key identifier from the HIAB certificate.
   - Information about HIAB usage (number of targets, number of scans).
   - MAC address.
   - List of installed rpm packages on the HIAB.

   ***Note**: The Update Package is bound to the generated key, i.e. it can only be uploaded on the specific HIAB on which the key was generated. Similarly, the key is bound to the HIAB on which it was generated.*

2. The information is signed and encrypted and then presented to the user.
3. The update key is then used on OUTSCAN to generate an update package.
4. The update key is validated on OUTSCAN to make sure that user has an active license.

   The update package contains:
   - An SQL file which updates the license information.
   - The key file with a unique key for the HIAB.
   - A file that updates vulnerability definitions.
   - A file that updates exploits information.
   - The list of installed packages send in the update key are compared with available packages, any packages that should be updated/installed are included in the update package.

5. The user uploads the update package on the HIAB.
6. The HIAB validate the key file in the package to make sure that the package is generated for this HIAB.
7. The vulnerability definitions and exploits information are inserted into the database.
8. The license information is updated in the database.
9. The rpm packages are installed/updated.
10. The HIAB is then restarted.