https://knowledge.rsasecurity.com/scolcms/set.aspx?id=8252

Rapid 7 NeXpose
RSA enVision Event Source

Configuration Instructions and Release Notes

Last Modified: Monday, October 31, 2011

Event Source (Device) Product Information	
Vendor	Rapid 7
Event Source (Device)	Rapid 7 NeXpose
Supported Versions	4.8
Additional Downloads	• For standard event source: sftpagent.conf.nexpose • For VAM source: sftpagent.conf.rapid7
enVision Product Information	
Version	3.7.1 and later
Event Source (Device) Type	nexpose, 696
Collection Method	File Reader
Event Source (Device) Class.Subclass	Security.Vulnerability
Content 2.0 Table	Vulnerability
Service	NIC File Reader Service

This document contains the following information for the Rapid 7 NeXpose event source:

Rapid 7 NeXpose Configuration Instructions

You can configure Rapid 7 NeXpose as either a VAM source or a standard event source.

Configure Rapid 7 NeXpose as a VAM Source

Rapid 7 NeXpose reports must be in the correct location and format for the RSA enVision platform to process them.

Important: The support for Rapid 7 NeXpose as a VAM source requires RSA enVision 4.0 Service Pack 4, Patch 4 or later, and bug fix (EBF)HF_ENV-35020_ENV-37260. For details, contact RSA enVision Customer Support.

To configure Rapid 7 NeXpose as a VAM source:

1. On the Rapid 7 NeXpose platform, set up the reports as follows:

    a. Navigate to the Reports tab on the NeXpose web console.

    b. When you create or edit a report, ensure that you set the report format as **NeXpose Simple XML Export**. This parameter can be found under General tab under Report Configuration.

    c. Note the output location for the report. By default, reports are output to the following location:

    `$`***`nexpose_dir`***`/nsc/htroot/reports/`***`xxxxxxxx`***

    where ***nexpose_dir*** is your NeXpose installation folder and ***xxxxxxxx*** is a system-generated number.

2. Apply bug fix HF_ENV-35020_ENV-37260. For details, contact RSA technical support.

3. On the RSA enVision platform, set up the NIC Asset Collector Service.

    a. Log on to the RSA enVision web UI.

    b. Select **Overview** > **System Configuration** > **Services** > **Asset Service** > **Manage Asset Collector Service**.

    c. Click **Add**.

    d. Fill in the fields as follows:

Parameter	Value
Collector Type	Rapid7
Directory Name	Enter any name for the folder. **Note:** Make sure to note this folder name. You use this folder name as part of the dir0.ftp parameter in step 4c.
Interval	Choose an interval, such as 1 minute.
Enabled	Select the check box

    e. Click **Apply**.

4. On the Rapid 7 NeXpose platform, install and configure the NIC SFTP Agent.

    a. Download or navigate to the **sftpagent.conf.rapid7** file.

    Note: The SFTP sample file is available on RSA SecurCare Online (SCOL) and on the enVision appliance. For details, see RSA enVision NIC SFTP Agent Sample Files.

    b. Save the SFTP configuration file as sftpagent.conf in the C:\NICsftpagent folder on the Rapid 7 NeXpose Server.

    c. Set the parameters for the source folder (on the Rapid 7 Server) and the destination folder (on the RSA enVision platform). For example, if the IP address of your RSA enVision appliance is 172.16.0.51, and your Rapid 7 Server is at IP address 1.1.1.1, then you should set the directory parameters as follows:

```
dir0=nexpose_dir/nsc/htroot/reports/xxxxxxxx
dir0.interval=60
dir0.compression=false
dir0.enabled=true
dir0.ftp=172.16.0.51,nic_sshd,publickey,asset_collector_folder_name_1.1.1
.1
```

    Note: Make sure to set the source folder for the reports (this is the **dir0** parameter) to the output location for the report on your NeXpose platform. This is the folder name that you saw in step 1c. Also, the ***asset_collector_folder_name*** is the name of the folder that you entered in step 3d.

Configure Rapid 7 NeXpose as a Standard Event Source

You must complete the following tasks to configure Rapid NeXpose to send logs to RSA enVision as a standard event source:

I. Configure Scripts

II. Set Up the NIC SFTP Agent

III. Set Up the NIC File Reader Service

Configure Scripts

To configure the scripts for NeXpose:

1. Create a new folder on your NeXpose host named, **C:\NeXposeScripts**
2. From the **/nexpose/scripts** folder in your Event Source Update installation directory, copy the **config.cfg** and **nexpose-audits.vbs** files, and paste them into **C:\NeXposeScripts**.
3. In the **nexpose-audits.vbs** file, edit the following parameter values.

Parameter	Value

Parameter	Value
FileName	***InstallPath*\nexpose\nse\nse.log**, where *InstallPath* is the location where NeXpose is installed, for example, C:\Program Files\rapid7.
FolderSize	**100**

4. Schedule the **nexpose-audits.vbs** file:
    a. Click **Start** > **Control Panel** > **Scheduled Tasks** > **Add Scheduled Task**.
    b. Click **Next**.
    c. Select **Command Prompt**, and click **Next**.
    d. In the **Name** field, type **rapid7Batch**.
    e. In the **Perform this task** field, select **Daily**, and click **Next**.
    f. Click **Next**.
    g. Enter your user name and password, and click **Next**.
    h. Ensure that **Open advanced propertied for this task when I click Finish** is selected, and click **Finish**.
    i. Select the **Task** tab.
    j. In the **Run** field, type **nexpose-audits.vbs**.
    k. In the **Start in** field, type **C:\NeXposeScripts**.
    l. Select the **Schedule** tab, click **Advanced**.
    m. Select **Repeat task**.
    n. Select **1 Minute**, and click **OK**.
    o. Click **Apply**, and enter your user name and password.
    p. Click **OK**.

[Back to Top]

Set Up the NIC SFTP Agent

To set up the NIC SFTP Agent:

1. Download or navigate to the **sftpagent.conf.nexpose** file.

    Note: The SFTP sample file is available on RSA SecurCare Online (SCOL) and on the enVision appliance. For details, see RSA enVision NIC SFTP Agent Sample Files.

2. Using the **sftpagent.conf.nexpose** file, set up the NIC SFTP Agent.

    For instructions on installing the **NIC SFTP Agent**, see RSA enVision NIC SFTP Agent Configuration.

[Back to Top]

Set Up the NIC File Reader Service

1. Log on to the RSA enVision web UI.
2. Select **Overview** > **System Configuration** > **Services** > **Device Service** > **Manage File Reader Service**.
3. Click **Add**.
4. In the **IP Address** field, enter the NeXpose device IP address.
5. From the **File Reader Type** field, select **nexpose**.
6. Click **Apply**.

[Back to Top]

Rapid 7 NeXpose Release Notes (20111031-165949)

What's New in This Release

RSA has added Rapid 7 NeXpose as a VAM source.

[Back to Top]

Rapid 7 NeXpose Release Notes (20110201-172305)

What's New in This Release

RSA has updated the configuration instructions for this release.

[Back to Top]

Rapid 7 NeXpose Release Notes (20101206-104928)

What's New in This Release

RSA has updated the configuration instructions for this release.

[Back to Top]