# Revision history

Copyright © 2015 Rapid7, LLC. Boston, Massachusetts, USA. All rights reserved. Rapid7 and Nexpose are trademarks of Rapid7, Inc. Other names appearing in this content may be trademarks of their respective owners.

For internal use only.

<table>
<thead>
<tr>
<th>Revision date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 10, 2014</td>
<td>Added revision history table.</td>
</tr>
<tr>
<td>January 5, 2015</td>
<td>Updated due to changes in the site configuration interface.</td>
</tr>
<tr>
<td>April 8, 2015</td>
<td>Nexpose 5.14: Updated product version.</td>
</tr>
<tr>
<td>June 24, 2015</td>
<td>Nexpose 5.15: Updated product version.</td>
</tr>
<tr>
<td>July 29, 2015</td>
<td>Nexpose 5.16: Updated product version.</td>
</tr>
<tr>
<td>August 26, 2015</td>
<td>Nexpose 5.17: Updated product version.</td>
</tr>
<tr>
<td>October 8, 2015</td>
<td>Nexpose 6.0: Updated to reflect new look and feel.</td>
</tr>
</tbody>
</table>
Discover

Find vulnerabilities in your environment.

Create a site

A site is a collection of assets to scan. You must have a site created before you can run a scan.

1. On the Home page, click Create Site.
   OR
   click the Create tab at the top and then select Site from the drop-down list.

   ![](Site listing panel - Create site button)

2. On the General page of the Site Configuration panel, enter a unique name for the site.

3. Click the Assets icon in the left navigation pane.

   **Tip:** A site configuration also includes a scan template, which defines the settings for the scan. You can see a list of scan templates by clicking Scan Setup in the Site Configuration panel. The default Full Audit template is good for first-time scans because it covers a large number of vulnerability checks. To make sure all the checks run, specify credentials. Another option is to use the Discovery Scan template, which collects basic information about each asset and does not require credentials, so you can get an overview of what you have.

4. In the Included Assets text box, enter one IP address or host name per line, or range of addresses separated by a hyphen. See the information box on the Assets page for examples.

5. Click Save & Scan.

   The Security Console displays the page for your scan, so you can watch its progress as it discovers assets and vulnerabilities.

   The new site also appears in the Site listing table of the Home page. A scan is in progress.
Eventually the scan completes. You can confirm that the scan has completed by looking at this table.
Assess

View and sort scan results to find out your security posture and remediation priorities.

You can drill down through scan data two different ways:

**Option A**

Click the **Vulnerabilities** icon to view and compare discovered vulnerabilities and then find out which assets are affected by each vulnerability. This approach is useful if you are concerned about specific vulnerabilities.

**Option B**

Click the **Assets** icon to see specific assets and then find out which vulnerabilities affect them. This approach is useful if you are concerned about certain sensitive assets. This guide shows the asset-based approach.
1. After a scan completes, click the **Assets** icon.

![Assets panel](image)

2. To see specific assets and find out which vulnerabilities affect them, select a viewing category.
3. Drill down to the subset of assets that you want to see.

4. Compare assets by different security metrics: Click column headings to sort assets by malware or exploit exposures, total vulnerabilities, or risk scores.

5. Click an asset’s IP address or host name to view details about it.
6. View details about the asset, including all discovered vulnerabilities.
   - To sort vulnerabilities by name, click the **Title** heading in the **Vulnerabilities** table.
   - To compare and prioritize vulnerabilities, click other column headings and sort them by different security metrics.

7. Click the name of a listed vulnerability to view details about it.
Vulnerability Listing details

The Security Console displays a page with details about the vulnerability, including its security metrics, affected assets, and remediation solutions.

Vulnerability details

8. Click the Back arrow on your browser to return to the asset details page.
Act

Create a report so that your organization can view its security posture and start to prioritize and remediate vulnerabilities.

You can start to create a report two different ways:

Option A

If you want to share urgent information about a sensitive asset, click on the Create dropdown menu on the top of the page for that asset, then click Report.

Option B

If you want to report on multiple assets, click the Reports icon. This guide shows the multiple-asset approach for creating an audit report in PDF format.

Home tool bar—Reports tab

1. Click the Reports icon.
   OR
   Click the Create tab at the top and then select Report from the drop-down list.
   The Reports page lists any reports that have been created.
   Click the New button.

Report panel—Create a Report tab
2. Select the **Audit Report** template. Each template controls what specific information is included in the report.

3. Select the **PDF** format under the *File format* dropdown menu.

4. Click **Select Sites, Assets**, or **Asset Groups** to view the **Select Report Scope** page.

5. Select **Assets** from the drop-down list.
6. Enter or select search criteria, and click Search. A list of assets is displayed.

7. Click check boxes for assets that you want to include in the reports, and click Done.

8. Click **Save and run the report** to generate the report. The Security Console displays the status of the report generation. When the report is complete, the creation date and time appear in the **View reports** page.

9. Click the report name to view the report.

The report shows remediation steps for each vulnerability on each asset.
3.3.1. ICMP timestamp response (generic-icmp-timestamp)

Description:
The remote host responded to an ICMP timestamp request. The ICMP timestamp response contains the remote host's date and time. This information could theoretically be used against some systems to exploit weak time-based random number generators in other services.

In addition, the versions of some operating systems can be accurately fingerprinted by analyzing their responses to invalid ICMP timestamp requests.

Affected Nodes:

<table>
<thead>
<tr>
<th>Affected Nodes</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.4.15.90</td>
<td>Able to determine remote system time</td>
</tr>
</tbody>
</table>

References:

<table>
<thead>
<tr>
<th>Source</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE</td>
<td>CVE-1999-0524</td>
</tr>
<tr>
<td>D2DB</td>
<td>95</td>
</tr>
<tr>
<td>XF</td>
<td>308</td>
</tr>
</tbody>
</table>

Vulnerability Solution:

- **HP-UX**
  - Disable ICMP timestamp responses on HP-UX
  - Execute the following command:
    ```
    add -i -s -d tcpip -p respond_to_timestamp_broadcast 0
    ```
  - The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

- **Cisco IOS**
  - Disable ICMP timestamp responses on Cisco IOS
  - Use ACLs to block ICMP types 13 and 14. For example:
    ```
    deny icmp any any 13
    deny icmp any any 14
    ```
  - Note that it is generally preferable to use ACLs that block everything by default and then selectively allow certain types of traffic in. For example, block everything and then only allow ICMP unreachable, ICMP echo reply, ICMP time exceeded, and ICMP source quench.
    ```
    permit icmp any any unreachable
    ```

Audit report-remediation steps

Tip: You can schedule reports to run automatically. This is useful if you create multiple sites and run scans on a regular basis. You can schedule reports to run after these scans are complete. To see scheduling options, click the **Schedule** tab in the *Report Configuration* panel.

10. Click the **View Reports** tab to access the report again, if you want to edit it or generate a new instance.
View reports tab-tools drop-down menu