



SOAR – Vulnerability Management

High-Volume Vulnerability Import

Document Version: 1.0.01

June 2017



Contents

| | |
|--|----|
| About this Guide----- | 3 |
| SOAR – Vulnerability Management ----- | 4 |
| Vulnerability Management Structure_____ | 4 |
| Object Types _____ | 5 |
| Record Types _____ | 5 |
| Set up Object Types, Record Types and Attributes ----- | 6 |
| Imports _____ | 7 |
| Review the Results ----- | 10 |

About this Guide

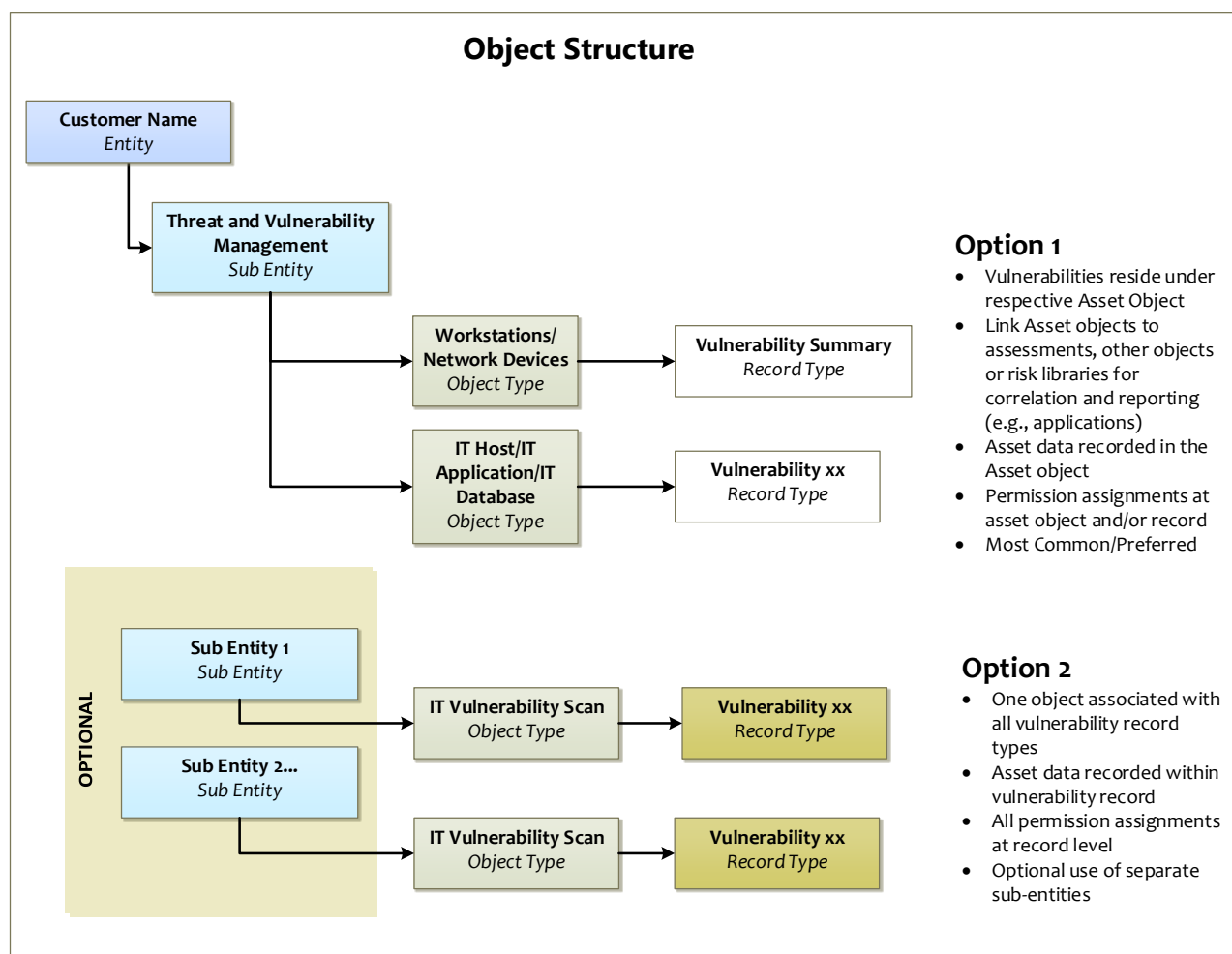
The Rsam Security Operations Analytics and Reporting (SOAR) – Vulnerability Management (VM) baseline configuration allows customers to automate, centralize and optimize the analysis, approval and reporting of asset and vulnerability data. The SOAR – VM baseline includes configurations for managing high volumes of vulnerabilities or findings that are discovered on workstations and other assets. This configuration streamlines your vulnerability management process by allowing assigned remediation teams to record one action plan per vulnerability that will address all affected devices (i.e. deploying a patch).

This guide provides information on how to use the pre-defined import configurations that will allow you to import high-volume vulnerability data into the module. It describes the pre-configured data structure for managing high-volume vulnerabilities and provides high-level guidance on how to import data into that structure successfully.

SOAR – Vulnerability Management

Vulnerability Management Structure

The High-Volume Vulnerability configuration structure uses a static “object” for each group of high-volume devices (as opposed to each individual asset) based on the scan results’ source. Upon import, scan results for a particular group will be consolidated to create a single record for each unique vulnerability (based on the unique ID defined in the import map), where each vulnerability record includes a list of all IP addresses and machine names reporting this vulnerability. This list is then used to calculate the number of devices affected by the vulnerability.



Object Types

The following object type has been pre-configured in the SOAR – VM module for your use:

| Object Type | Description |
|------------------------------|--|
| Workstations/Network Devices | A standard object that uses one object per group of workstations or network devices (commonly grouped by type, location, or scan). This object comprises a summary of workstation or network device vulnerabilities that are populated using an import file. |

Record Types

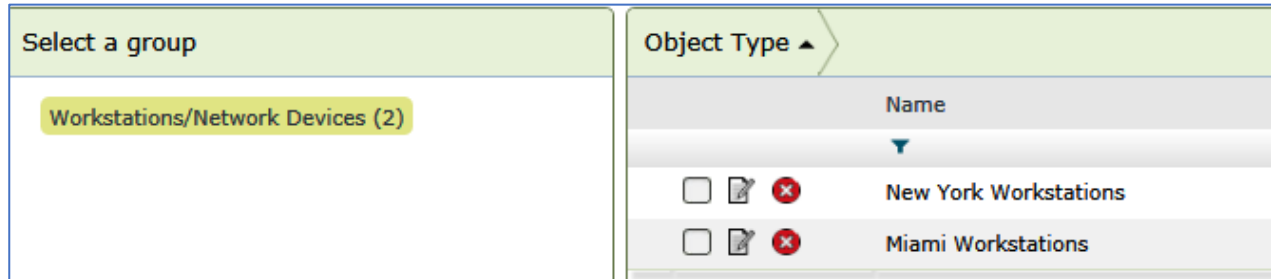
The following record type has been pre-configured in this SOAR – VM module for your use:

| Record Type | Description |
|-------------------------|--|
| Vulnerability - Summary | One record per vulnerability ID per workstation group. Each record includes the count of devices containing vulnerability(s) plus a list of IP addresses and DNS names of the effected devices. These records are automatically created during imports. They are generated based on a unique ID that commonly consists of vulnerability ID + Port. |

If a high-volume vulnerability import is used (i.e., workstation vulnerabilities), these are mapped to a static, applicable Workstations/Network Devices object as defined on the **General** tab of Import Records interface. All vulnerabilities begin in the “Open” workflow state.

Set up Object Types, Record Types and Attributes

1. Create a separate object of type “Workstations/Network Devices,” for each workstation grouping. For example, if you want to run scans for workstations in New York and Miami, create 2 separate objects – “New York Workstations” and “Miami Workstations”. The objects should be placed under the sub entity of your choice.



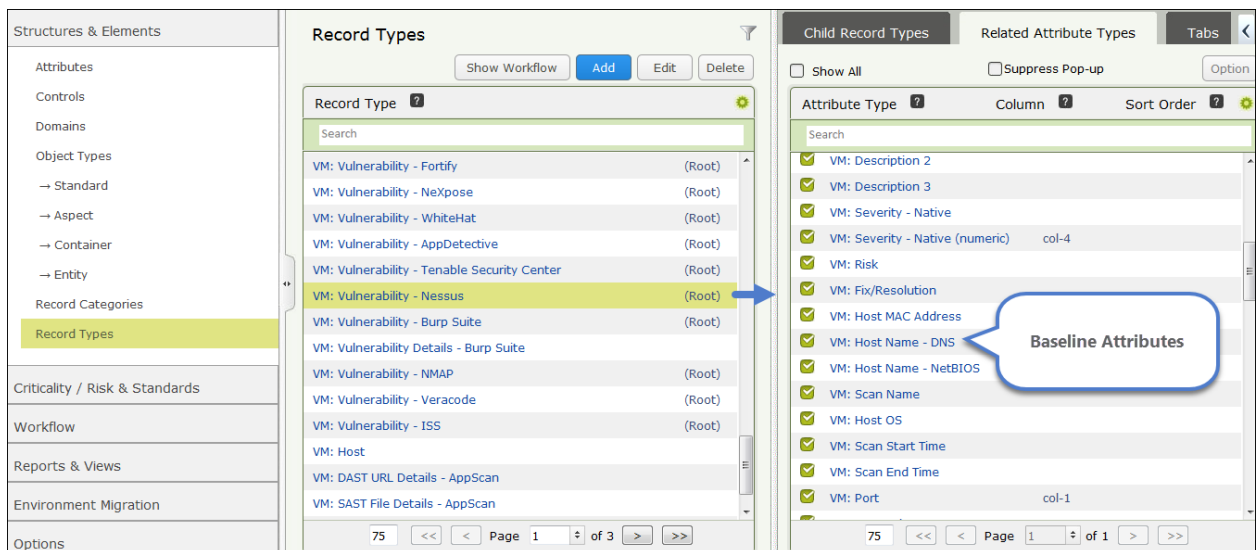
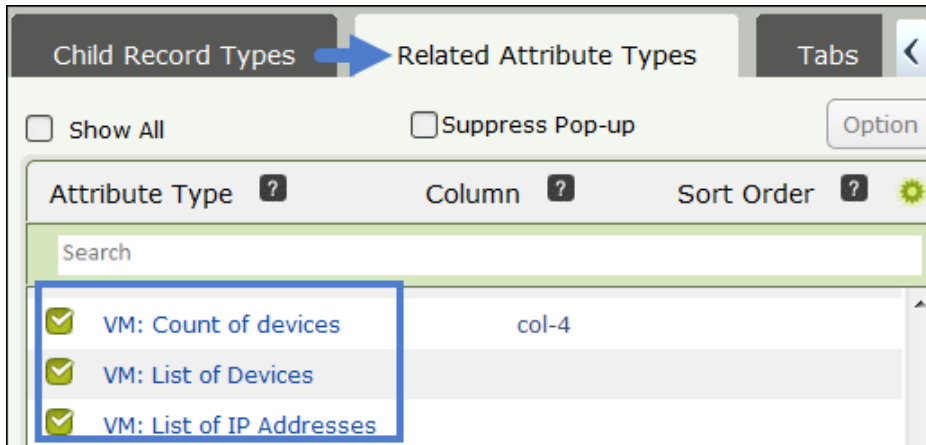
2. The baseline includes the high-volume configuration for Qualys vulnerabilities. To use this configuration for non-Qualys vulnerabilities, you can modify the existing “VM: Qualys VM Summary” record type. Rename the “Vulnerability - Qualys VM Summary” record category and “Vulnerability - Qualys VM Summary” record type to match your data source.

Alternatively, you can create a new record category/type if your Rsam license allows you to create custom record type and record category. If you have created a new record category, be sure to associate it with the Workstations/Network Devices object type.

3. Associate necessary attributes to your record type. The following considerations should be kept in mind when you are selecting attributes:
 - a. Only include vulnerability-related attributes that are reported in the scan data result set you will be importing into Rsam.
 - b. Only include attributes where the data reported for each vulnerability ID is going to be identical across the summarized vulnerabilities. If imported data may contain a unique response for each of the summarized records, it should not be included. For example, “VM: Actual Result” cannot be mapped in a summary record since each of the summarized vulnerabilities may report a different value.

The following attributes must be linked to the record type:

- List of IP Addresses
- List of Devices
- Count of Devices



Imports

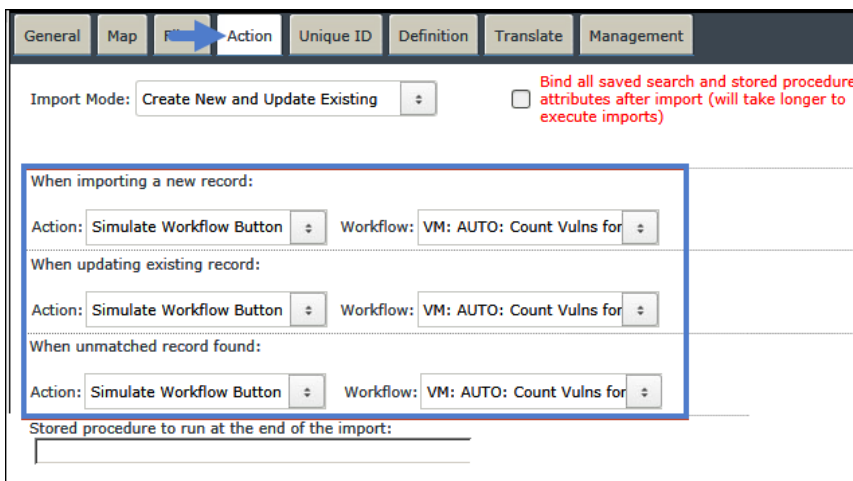
When your object type, record category, record type, and attributes are available, you are ready to import the vulnerabilities. This section will walk you through the high-level steps for importing vulnerabilities.

1. Create one import file from your data source for each workstation scan object created in step #1 above.
2. Create separate record import map for each workstation vulnerability scan object. As an example, please refer to the “V: Qualys_Summary_XML” map.
3. To import vulnerabilities, the following configurations must be set properly.
 - a. Map the “List of IP addresses” and “List of Devices” attributes in the APPEND mode.

| LN/ | XML ELEMENT | MODE | RSAM ELEMENT | RSAM TYPE |
|-----|-------------|-----------|----------------------|----------------|
| LN/ | DIAGNOSIS | OVERWRITE | Description | Attribute Type |
| LN/ | CONSE | OVERWRITE | Risk | Attribute Type |
| | value | APPEND | List of IP Addresses | Attribute Type |
| | name | APPEND | List of Devices | Attribute Type |

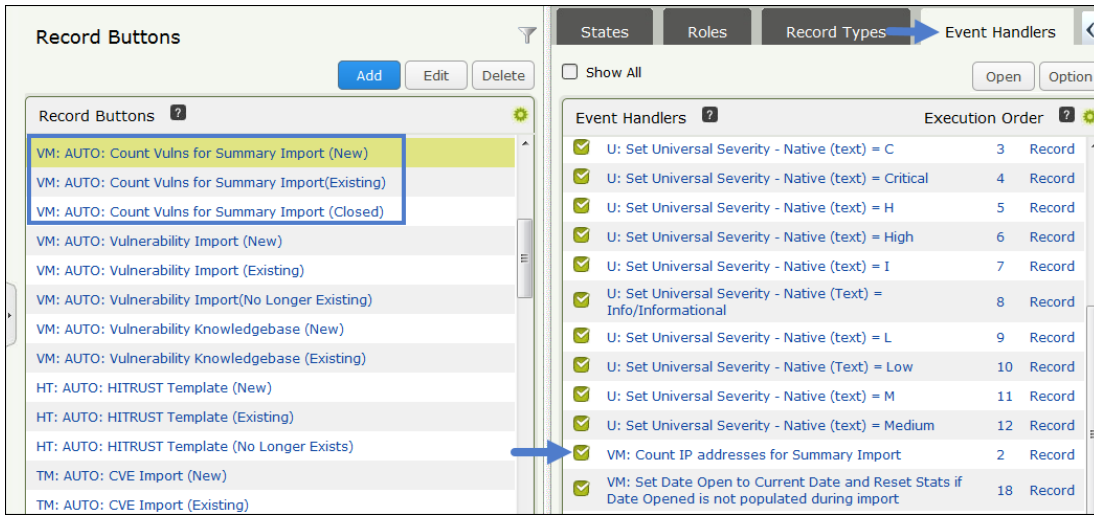
- b. On the **Actions** tab of the Import screen, select the Action and Workflow combination for each case mentioned in the table below:

| Case I | Action | Workflow |
|-------------------------------|--------------------------|---|
| When importing a new record | Simulate Workflow Button | AUTO: Count Vulns for Summary Import (New) |
| When updating existing record | Simulate Workflow Button | AUTO: Count Vulns for Summary Import (Existing) |
| When unmatched record found | Simulate Workflow Button | AUTO: Count Vulns for Summary Import (Closed) |



The “VM: Count IP addresses for Summary import” handler must be linked to the AUTO: Count Vulns for Summary Import (New) and AUTO: Count Vulns for Summary Import (Existing) buttons.

This handler executes the stored procedure required to calculate the number of affected devices.

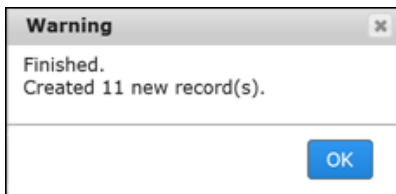


The screenshot shows the 'Record Buttons' and 'Event Handlers' sections of the R-sam interface. The 'Record Buttons' section on the left lists various import templates. The 'Event Handlers' section on the right shows a list of handlers with their execution order. A blue arrow points to the handler 'VM: Count IP addresses for Summary Import' which is at execution order 2.

| Event Handler | Execution Order | Status |
|---|-----------------|--------|
| U: Set Universal Severity - Native (text) = C | 3 | Record |
| U: Set Universal Severity - Native (text) = Critical | 4 | Record |
| U: Set Universal Severity - Native (text) = H | 5 | Record |
| U: Set Universal Severity - Native (text) = High | 6 | Record |
| U: Set Universal Severity - Native (text) = I | 7 | Record |
| U: Set Universal Severity - Native (Text) = Info/Informational | 8 | Record |
| U: Set Universal Severity - Native (text) = L | 9 | Record |
| U: Set Universal Severity - Native (Text) = Low | 10 | Record |
| U: Set Universal Severity - Native (text) = M | 11 | Record |
| U: Set Universal Severity - Native (text) = Medium | 12 | Record |
| VM: Count IP addresses for Summary Import | 2 | Record |
| VM: Set Date Open to Current Date and Reset Stats if Date Opened is not populated during import | 18 | Record |

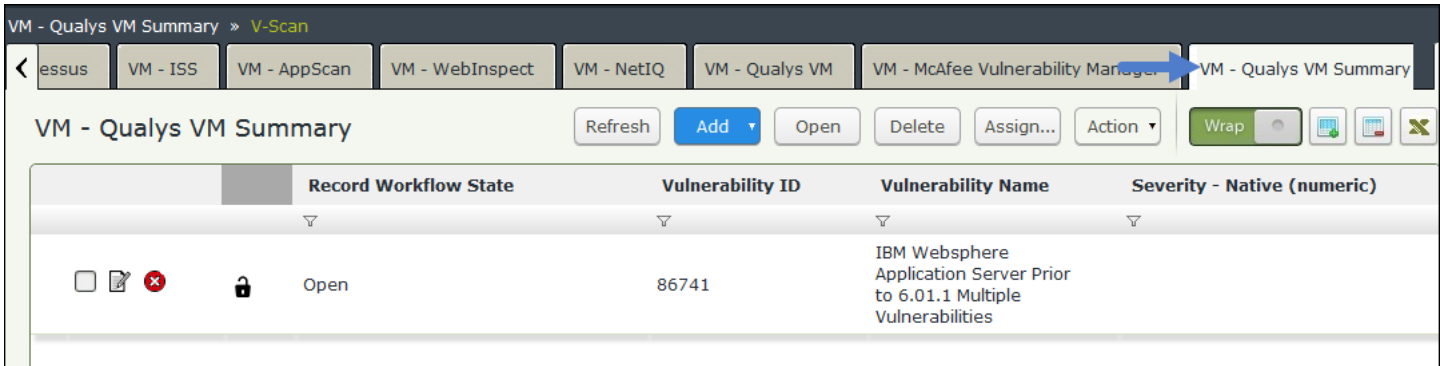
Note: Subsequent imports overwrite the IP List (does not continue to append) and recalculate the number of effected devices. Therefore, all workstation scan results for a given scan object must be contained within one import file.

- Complete the import to generate new records, or update the existing ones.



Review the Results

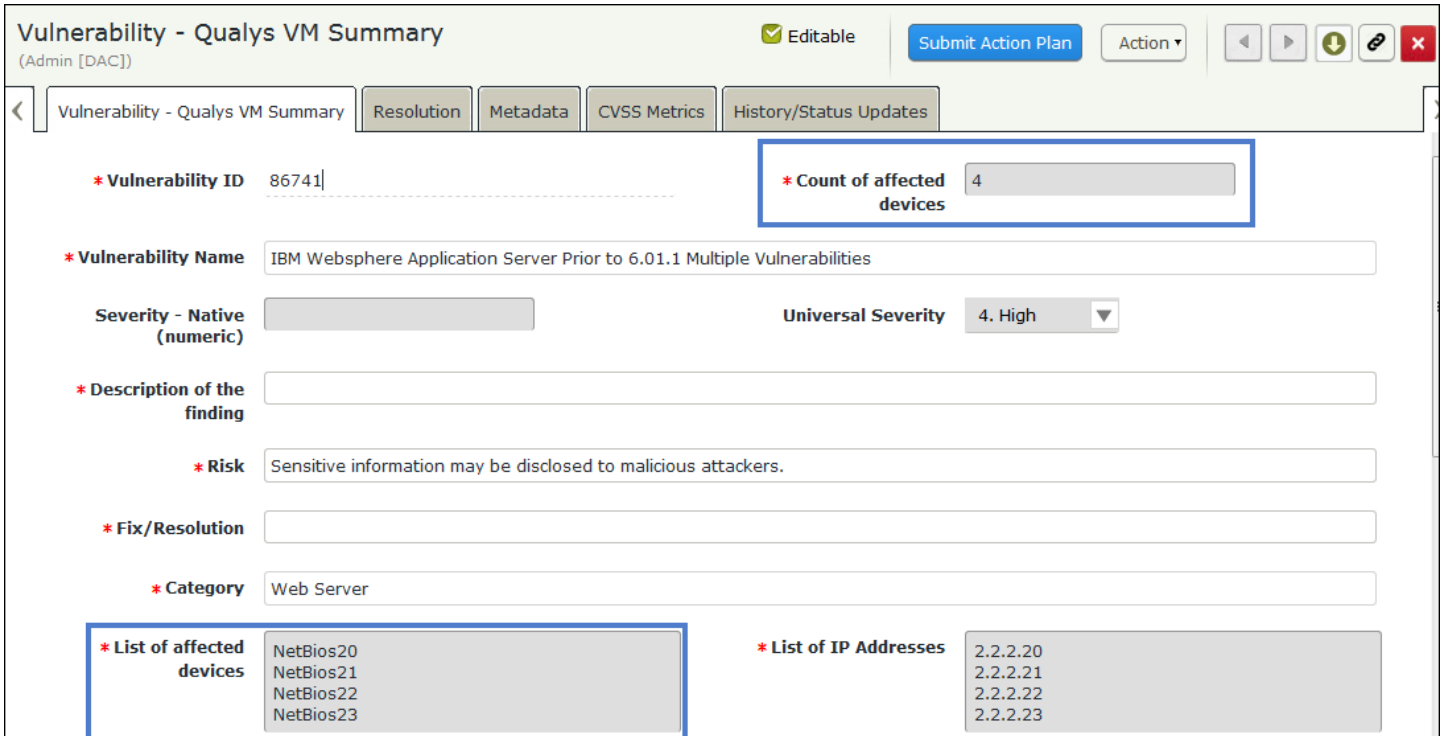
After you complete the import successfully, you can review the import results by navigating to **Record > Open By Category > VM – Qualys VM Summary**.



The screenshot shows a table with the following columns: Record Workflow State, Vulnerability ID, Vulnerability Name, and Severity - Native (numeric). A single record is visible with the following details:

| Record Workflow State | Vulnerability ID | Vulnerability Name | Severity - Native (numeric) |
|-----------------------|------------------|---|-----------------------------|
| Open | 86741 | IBM Websphere Application Server Prior to 6.01.1 Multiple Vulnerabilities | |

Double-click on a vulnerability record to open its details. The vulnerability record will contain a list of devices that are affected by that vulnerability. For example, the image below illustrates the vulnerability ID#86741 and the effected devices.



The screenshot shows the details for vulnerability ID 86741. The page includes the following fields and sections:

- Vulnerability ID:** 86741
- Count of affected devices:** 4
- Vulnerability Name:** IBM Websphere Application Server Prior to 6.01.1 Multiple Vulnerabilities
- Severity - Native (numeric):** [Empty]
- Universal Severity:** 4. High
- Description of the finding:** [Empty]
- Risk:** Sensitive information may be disclosed to malicious attackers.
- Fix/Resolution:** [Empty]
- Category:** Web Server
- List of affected devices:** NetBios20, NetBios21, NetBios22, NetBios23
- List of IP Addresses:** 2.2.2.20, 2.2.2.21, 2.2.2.22, 2.2.2.23