# Qualys Enterprise TruRisk™ Platform

## Limited Customer Release Notes

Version 10.35.2-2

September 02, 2025 (Updated on November 07, 2025)

### What's New?

Vulnerability Management

Support for Kernel Live Patching on Linux Systems

## Contents

# Support for Kernel Live Patching on Linux Systems

## Introduction

Linux kernel live patching allows critical and important security fixes to be applied to a running kernel without requiring a reboot or service downtime. This ensures that systems remain protected against newly disclosed vulnerabilities while maintaining uptime and operational continuity. Unlike full kernel updates, live patches specifically target security flaws, enabling administrators to apply fixes immediately while deferring full system reboots to planned maintenance windows.

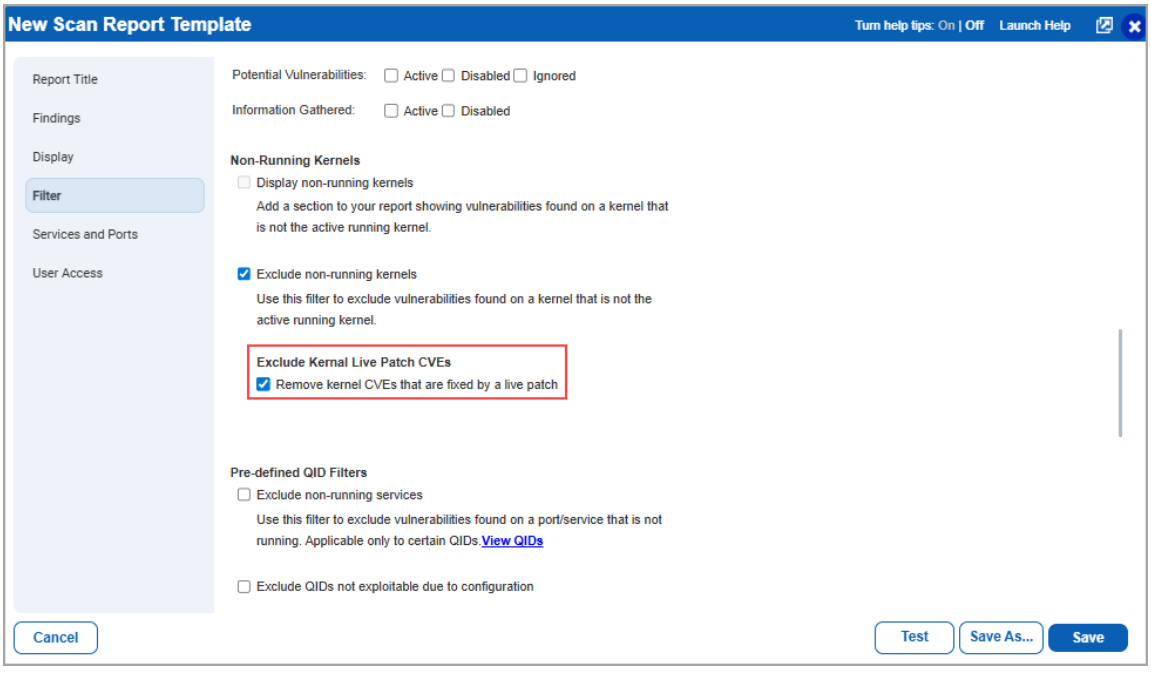
However, in the current detection process, vulnerabilities fixed through live patches still appear in reports as unresolved because assessments are performed only against the baseline kernel version. This creates false positives, adding complication to vulnerability reports and increasing users effort in triaging.

## UI Changes

Earlier, all the vulnerabilities were detected based on the baseline kernel version, including the kernel CVEs that are fixed by live patches for critical and important vulnerabilities. You were able to view the vulnerabilities marked as open even when they were already fixed by live patches. This led to false positives, making it difficult to identify which CVEs had already been addressed by live patches.

With this release, you can now filter/remove kernel CVEs that are fixed by a live patch. To filter the fixed CVEs, we have introduced a new checkbox, and you can view this by navigating to:

1. **Reports** > **Templates** > **New** > **Scan Template**
   **A New Scan Report Template** window is displayed.
2. In **Filter**, select **Exclude non-running kernels** > select **Remove kernel CVEs that are fixed by a live patch** under **Exclude Kernel Live patch CVEs**.
3. Click **Save**.



**Notes:**

- This feature is applicable only if you have a VMRS and VMSP enabled account.
- **Remove kernel CVEs that are fixed by a live patch** checkbox is visible only if you have selected the **Exclude non-running kernels**. So, ensure to select **Exclude non-running kernels** checkbox.

Once you select the checkbox, it is saved in the report template. When you launch a host based scan report, all the live patched CVES are excluded and will not be visible in the report generated. You can view only the CVEs that are not yet patched. For example, a security advisory may cover N number of CVEs, but the live patch covers fixes only for critical/important CVEs.

For example, consider the following scenarios:

- RHSA-2022:7110 covers 7 CVEs, but a live patch is available for only one - CVE-2022-2588. In the report, you can see all the remaining CVEs that are not patched and still exist.
- If a QID has 7 CVEs and the live patch is available for all 7 CVEs, then that particular QID will not be visible in the report.

**Note:** This is only applicable for Host-Based Scan Report, and it supports only CSV file format.

### Benefits of filtering Live patched CVEs

- **Accurate Reporting:** Eliminates false positives by filtering out CVEs already fixed by live patches, giving users a true picture of their risk posture.
- **Reduced Operational Overhead:** Security teams save time by focusing only on real, unpatched vulnerabilities instead of manually validating live-patched CVEs.
- **Improved Security Confidence:** Ensures users know exactly which vulnerabilities remain a threat, strengthening trust in security reporting.
- **Seamless Extension Across Platforms:** As most major Linux distributions support live patching, this feature provides broad coverage and consistent value across environments.

## API Changes

### Scan Template API: Report Template updates to remove Live Patched CVEs

| New or Updated API | Updated |
|---|---|
| API Endpoint | /api/5.0/fo/report/template/scan/ |
| Method | POST, GET |
| DTD or XSD Changes | Yes |

With this release, you can now create, update, and export a scan report template to remove all the live patched CVEs. We have implemented versioning and introduced a new parameter. This new input parameter is applicable only to v5.0 version.

**Input Parameter:**

| Parameter | Required/ Optional | Data Type | Description |
|---|---|---|---|
| exclude_kpatch_cve ={0\|1} | Required | Integer | Specify 1 to remove kernel CVEs that are fixed by a live patch |

**Note:** This is only applicable for Host-Based Scan Report, and it supports only CSV file format.

### Sample - Create a scan report template

**API Request:**

```
curl --location 'https://
<qualys_base_url>/api/5.0/fo/report/template/scan/?action=create&report_format=xml' \
--header 'Accept: */*' \
--header 'X-Requested-With: curl' \
--header 'content-type: text/xml' \
--header 'Authorization: Bearer <JWT Token>' \
```

**API Response:**

```
<?xml version="1.0" encoding="UTF-8" ?>
<REPORTTEMPLATE>
	<SCANTEMPLATE>
		<TITLE>
			<INFO key="title">
				<![CDATA[AP0f_PT]]>
			</INFO>
		</TITLE>
		<TARGET>
			<INFO key="scan_selection">HostBased</INFO>
			<INFO key="ips">
				<![CDATA[ ]]>
			</INFO>
			<INFO key="asset_groups">
				<![CDATA[all]]>
			</INFO>
			<INFO key="tag_set_by">
				<![CDATA[ id ]]>
			</INFO>
		</TARGET>
		<DISPLAY>
			<INFO key="display_text_summary">
				<![CDATA[1]]>
			</INFO>
			<INFO key="graph_severity">
				<![CDATA[0]]>
			</INFO>
			<INFO key="graph_potential_severity">
				<![CDATA[0]]>
			</INFO>
			<INFO key="graph_ig_severity">
				<![CDATA[0]]>
			</INFO>
			<INFO key="graph_os">
				<![CDATA[0]]>
```

```
</INFO>
<INFO key="graph_services">
        <![CDATA[0]]>
</INFO>
<INFO key="display_custom_footer">
        <![CDATA[0]]>
</INFO>
<INFO key="display_custom_footer_text">
        <![CDATA[]]>
</INFO>
<INFO key="sort_by">
        <![CDATA[host]]>
</INFO>
<INFO key="cvss">
        <![CDATA[all]]>
</INFO>
<INFO key="qualys_system_ids">
        <![CDATA[0]]>
</INFO>
<INFO key="include_vuln_details">
        <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_threat">
        <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_impact">
        <![CDATA[0]]>
</INFO>
<INFO key="include_vuln_details_solution">
        <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_compliance">
        <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_exploit">
        <![CDATA[0]]>
</INFO>
<INFO key="include_vuln_details_malware">
        <![CDATA[0]]>
</INFO>
<INFO key="include_vuln_details_results">
        <![CDATA[0]]>
</INFO>
<INFO key="include_vuln_details_appendix">
        <![CDATA[1]]>
</INFO>
<INFO key="exclude_account_id">
        <![CDATA[0]]>
</INFO>
<INFO key="metadata_ec2_instances">
        <![CDATA[0]]>
</INFO>
<INFO key="cloud_provider_metadata">
        <![CDATA[0]]>
</INFO>
```

```
            <INFO key="include_vuln_details_detection_logic">
                <![CDATA[0]]>
            </INFO>
            <INFO key="vuln_detection_source">
                <![CDATA[1]]>
            </INFO>
            <INFO key="trurisk_elimination_status">
                <![CDATA[0]]>
            </INFO>
            <INFO key="mitre_attack_details">
                <![CDATA[1]]>
            </INFO>
        </DISPLAY>
        <FILTER>
            <INFO key="selective_vulns">
                <![CDATA[complete]]>
            </INFO>
            <!-- For correct deployment with script set searchlist id to VISTA_SL_ID -->
            <!-- <INFO key="search_list_ids">
            <![CDATA[1574272]]></INFO> -->
            <INFO key="exclude_qid_option">
                <![CDATA[0]]>
            </INFO>
            <INFO key="exclude_search_list_ids">
                <![CDATA[1574322]]>
            </INFO>
            <INFO key="included_os">
                <![CDATA[ALL]]>
            </INFO>
            <INFO key="status_new">
                <![CDATA[1]]>
            </INFO>
            <INFO key="status_active">
                <![CDATA[1]]>
            </INFO>
            <INFO key="status_reopen">
                <![CDATA[1]]>
            </INFO>
            <INFO key="status_fixed">
                <![CDATA[1]]>
            </INFO>
            <INFO key="vuln_active">
                <![CDATA[1]]>
            </INFO>
            <INFO key="vuln_disabled">
                <![CDATA[0]]>
            </INFO>
            <INFO key="vuln_ignored">
                <![CDATA[0]]>
            </INFO>
            <INFO key="potential_active">
                <![CDATA[1]]>
            </INFO>
            <INFO key="potential_disabled">
                <![CDATA[0]]>
```

```
                </INFO>
                <INFO key="potential_ignored">
                        <![CDATA[0]]>
                </INFO>
                <INFO key="ig_active">
                        <![CDATA[1]]>
                </INFO>
                <INFO key="ig_disabled">
                        <![CDATA[0]]>
                </INFO>
                <INFO key="ig_ignored">
                        <![CDATA[0]]>
                </INFO>
                <INFO key="display_non_running_kernels">
                        <![CDATA[0]]>
                </INFO>
                <INFO key="exclude_non_running_kernel">
                        <![CDATA[1]]>
                </INFO>
                <INFO key="exclude_non_running_services">
                        <![CDATA[1]]>
                </INFO>
                <INFO key="exclude_kpatch_cve">
                        <![CDATA[ 1 ]]>
                </INFO>
                <INFO key="exclude_superceded_patches">
                        <![CDATA[0]]>
                </INFO>
                <INFO key="exclude_qids_not_exploitable_due_to_configuration">
                        <![CDATA[0]]>
                </INFO>
                <INFO key="categories_list">
                        <![CDATA[ALL]]>
                </INFO>
        </FILTER>
        <SERVICESPORTS>
                <INFO key="required_services">
                        <![CDATA[]]>
                </INFO>
                <INFO key="unauthorized_services">
                        <![CDATA[]]>
                </INFO>
                <INFO key="services_info">
                        <![CDATA[]]>
                </INFO>
                <INFO key="required_ports">
                        <![CDATA[]]>
                </INFO>
                <INFO key="unauthorized_ports">
                        <![CDATA[]]>
                </INFO>
        </SERVICESPORTS>
        <USERACCESS>
                <INFO key="report_access_users">
                        <![CDATA[]]>
```

```
                        </INFO>
                        <INFO key="global">
                                <![CDATA[0]]>
                        </INFO>
                </USERACCESS>
        </SCANTEMPLATE>
</REPORTTEMPLATE>'
```

**DTD Output**

```
<!-- QUALYS SIMPLE_RETURN DTD -->
<!ELEMENT SIMPLE_RETURN (REQUEST?,RESPONSE)>
<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
<!-- If specified, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>
<!ELEMENT RESPONSE (DATETIME, CODE?, TEXT, ITEM_LIST?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT ITEM_LIST (ITEM+)>
<!ELEMENT ITEM (KEY, VALUE*)>
<!-- EOF -->
```

### Sample – Update a scan report template

**API Request:**

```
curl --location
'https://<qualys_base_url>/api/5.0/fo/report/template/scan/?action=update&report_format=xml
&template_id=3415298' \
--header 'Accept: */*' \
--header 'X-Requested-With: curl' \
--header 'content-type: text/xml' \
--header 'Authorization: Bearer <JWT Token>' \
```

**API Response:**

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORTTEMPLATE SYSTEM "https://
<qualys_base_url>/api/2.0/fo/report/template/scan/scanreporttemplate_info.dtd">
        <REPORTTEMPLATE>
                <SCANTEMPLATE>
                        <TITLE>
                                <INFO key="title">
                                        <![CDATA[TrendingTimeframe_SingleIP_AllData]]>
                                </INFO>
                                <!-->
                                <INFO key="owner">
                                        <![CDATA[1082593]]></INFO>-->
                                </TITLE>
```

```
<TARGET>
        <INFO key="scan_selection">
                <![CDATA[HostBased]]>
        </INFO>
        <INFO key="include_trending">
                <![CDATA[1]]>
        </INFO>
        <INFO key="selection_type">
                <![CDATA[days]]>
        </INFO>
        <INFO key="selection_range">
                <![CDATA[15]]>
        </INFO>
        <INFO key="limit_timeframe">
                <![CDATA[0]]>
        </INFO>
        <INFO key="asset_groups">
                <![CDATA[]]>
        </INFO>
        <INFO key="network">
                <![CDATA[-100]]>
        </INFO>
        <INFO key="ips">
                <![CDATA[ ]]>
        </INFO>
        <INFO key="host_with_cloud_agents">
                <![CDATA[all]]>
        </INFO>
</TARGET>
<DISPLAY>
        <INFO key="graph_business_risk">
                <![CDATA[0]]>
        </INFO>
        <INFO key="graph_vuln_over_time">
                <![CDATA[0]]>
        </INFO>
        <INFO key="display_text_summary">
                <![CDATA[1]]>
        </INFO>
        <INFO key="graph_status">
                <![CDATA[0]]>
        </INFO>
        <INFO key="graph_potential_status">
                <![CDATA[0]]>
        </INFO>
        <INFO key="graph_severity">
                <![CDATA[0]]>
        </INFO>
        <INFO key="graph_potential_severity">
                <![CDATA[0]]>
        </INFO>
        <INFO key="graph_ig_severity">
                <![CDATA[0]]>
        </INFO>
        <INFO key="graph_top_categories">
```

<![CDATA[0]]>
</INFO>
<INFO key="graph_top_vulns">
<![CDATA[0]]>
</INFO>
<INFO key="graph_os">
<![CDATA[0]]>
</INFO>
<INFO key="graph_services">
<![CDATA[0]]>
</INFO>
<INFO key="graph_top_ports">
<![CDATA[0]]>
</INFO>
<INFO key="display_custom_footer">
<![CDATA[0]]>
</INFO>
<INFO key="display_custom_footer_text">
<![CDATA[]]>
</INFO>
<INFO key="sort_by">
<![CDATA[host]]>
</INFO>
<INFO key="host_details">
<![CDATA[1]]>
</INFO>
<INFO key="host_ag_details">
<![CDATA[1]]>
</INFO>
<INFO key="qualys_system_ids">
<![CDATA[1]]>
</INFO>
<INFO key="include_text_summary">
<![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details">
<![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_threat">
<![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_impact">
<![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_solution">
<![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_vpatch">
<![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_compliance">
<![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_exploit">
<![CDATA[1]]>

```
                </INFO>
                <INFO key="include_vuln_details_malware">
                        <![CDATA[1]]>
                </INFO>
                <INFO key="include_vuln_details_results">
                        <![CDATA[1]]>
                </INFO>
                <INFO key="include_vuln_details_appendix">
                        <![CDATA[0]]>
                </INFO>
                <INFO key="exclude_account_id">
                        <![CDATA[0]]>
                </INFO>
                <INFO key="include_vuln_details_reopened">
                        <![CDATA[1]]>
                </INFO>
                <INFO key="metadata_ec2_instances">
                        <![CDATA[1]]>
                </INFO>
                <INFO key="cloud_provider_metadata">
                        <![CDATA[1]]>
                </INFO>
                <INFO key="include_vuln_details_detection_logic">
                        <![CDATA[1]]>
                </INFO>
        </DISPLAY>
        <FILTER>
                <INFO key="selective_vulns">
                        <![CDATA[complete]]>
                </INFO>
                <INFO key="search_list_ids">
                        <![CDATA[]]>
                </INFO>
                <INFO key="exclude_qid_option">
                        <![CDATA[0]]>
                </INFO>
                <INFO key="exclude_search_list_ids">
                        <![CDATA[]]>
                </INFO>
                <INFO key="included_os">
                        <![CDATA[ALL]]>
                </INFO>
                <INFO key="status_new">
                        <![CDATA[1]]>
                </INFO>
                <INFO key="status_active">
                        <![CDATA[1]]>
                </INFO>
                <INFO key="status_reopen">
                        <![CDATA[1]]>
                </INFO>
                <INFO key="status_fixed">
                        <![CDATA[1]]>
                </INFO>
                <INFO key="vuln_active">
```

```
                                        <![CDATA[1]]>
                                    </INFO>
                                    <INFO key="vuln_disabled">
                                        <![CDATA[1]]>
                                    </INFO>
                                    <INFO key="vuln_ignored">
                                        <![CDATA[1]]>
                                    </INFO>
                                    <INFO key="potential_active">
                                        <![CDATA[1]]>
                                    </INFO>
                                    <INFO key="potential_disabled">
                                        <![CDATA[1]]>
                                    </INFO>
                                    <INFO key="potential_ignored">
                                        <![CDATA[1]]>
                                    </INFO>
                                    <INFO key="ig_active">
                                        <![CDATA[1]]>
                                    </INFO>
                                    <INFO key="ig_disabled">
                                        <![CDATA[1]]>
                                    </INFO>
                                    <INFO key="ig_ignored">
                                        <![CDATA[0]]>
                                    </INFO>
                                    <INFO key="display_non_running_kernels">
                                        <![CDATA[0]]>
                                    </INFO>
                                    <INFO key="exclude_non_running_kernel">
                                        <![CDATA[1]]>
                                    </INFO>
                                    <INFO key="exclude_kpatch_cve">
                                        <![CDATA[ 1 ]]>
                                    </INFO>
                                    <INFO key="exclude_non_running_services">
                                        <![CDATA[1]]>
                                    </INFO>
                                    <INFO key="exclude_superceded_patches">
                                        <![CDATA[0]]>
                                    </INFO>
                                    <INFO
key="exclude_qids_not_exploitable_due_to_configuration">
                                        <![CDATA[0]]>
                                    </INFO>
                                    <INFO key="categories_list">
                                        <![CDATA[ALL]]>
                                    </INFO>
                                </FILTER>
                                <SERVICESPORTS>
                                    <INFO key="required_services">
                                        <![CDATA[]]>
                                    </INFO>
                                    <INFO key="unauthorized_services">
                                        <![CDATA[]]>
```

```
                    </INFO>
                    <INFO key="services_info">
                        <![CDATA[]]>
                    </INFO>
                    <INFO key="required_ports">
                        <![CDATA[]]>
                    </INFO>
                    <INFO key="unauthorized_ports">
                        <![CDATA[]]>
                    </INFO>
                </SERVICESPORTS>
                <USERACCESS>
                    <!-->
                    <INFO key="report_access_users">
                        <![CDATA[]]></INFO>-->
                        <INFO key="global">
                            <![CDATA[1]]>
                        </INFO>
                    </USERACCESS>
                </SCANTEMPLATE>
            </REPORTTEMPLATE>
```

**DTD Output:**

```
 <!-- QUALYS SIMPLE_RETURN DTD -->
<!ELEMENT SIMPLE_RETURN (REQUEST?,RESPONSE)>
<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
<!-- If specified, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>
<!ELEMENT RESPONSE (DATETIME, CODE?, TEXT, ITEM_LIST?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT ITEM_LIST (ITEM+)>
<!ELEMENT ITEM (KEY, VALUE*)>
<!-- EOF -->
```

### Sample - Export a scan report template

**API Request:**

```
curl --location
'https://<qualys_base_url>/api/5.0/fo/report/template/scan/?action=export&report_format=xml
&template_id=3415298' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Bearer <JWT Token>'
```

**API Response:**

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORTTEMPLATE SYSTEM
"https://<qualys_base_url>/api/5.0/fo/report/template/scan/scanreporttemplate_info.dtd">
<REPORTTEMPLATE>
   <SCANTEMPLATE>
      <TITLE>
         <INFO key="template_id">
            <![CDATA[3415298]]>
         </INFO>
         <INFO key="title">
            <![CDATA[TrendingTimeframe_SingleIP_AllData]]>
         </INFO>
         <INFO key="owner">
            <![CDATA[1049963]]>
         </INFO>
      </TITLE>
      <TARGET>
         <INFO key="scan_selection">
            <![CDATA[HostBased]]>
         </INFO>
         <INFO key="include_trending">
            <![CDATA[1]]>
         </INFO>
         <INFO key="selection_type">
            <![CDATA[days]]>
         </INFO>
         <INFO key="selection_range">
            <![CDATA[15]]>
         </INFO>
         <INFO key="limit_timeframe">
            <![CDATA[0]]>
         </INFO>
         <INFO key="asset_groups">
            <![CDATA[]]>
         </INFO>
         <INFO key="network">
            <![CDATA[-100]]>
         </INFO>
         <INFO key="ips">
            <![CDATA[]]>
         </INFO>
         <INFO key="host_with_cloud_agents">
            <![CDATA[all]]>
         </INFO>
      </TARGET>
      <DISPLAY>
         <INFO key="graph_business_risk">
            <![CDATA[0]]>
         </INFO>
         <INFO key="graph_vuln_over_time">
            <![CDATA[0]]>
         </INFO>
         <INFO key="display_text_summary">
```

```
    <![CDATA[1]]>
  </INFO>
  <INFO key="graph_status">
    <![CDATA[0]]>
  </INFO>
  <INFO key="graph_potential_status">
    <![CDATA[0]]>
  </INFO>
  <INFO key="graph_severity">
    <![CDATA[0]]>
  </INFO>
  <INFO key="graph_potential_severity">
    <![CDATA[0]]>
  </INFO>
  <INFO key="graph_ig_severity">
    <![CDATA[0]]>
  </INFO>
  <INFO key="graph_top_categories">
    <![CDATA[0]]>
  </INFO>
  <INFO key="graph_top_vulns">
    <![CDATA[0]]>
  </INFO>
  <INFO key="graph_os">
    <![CDATA[0]]>
  </INFO>
  <INFO key="graph_services">
    <![CDATA[0]]>
  </INFO>
  <INFO key="graph_top_ports">
    <![CDATA[0]]>
  </INFO>
  <INFO key="display_custom_footer">
    <![CDATA[0]]>
  </INFO>
  <INFO key="display_custom_footer_text">
    <![CDATA[]]>
  </INFO>
  <INFO key="sort_by">
    <![CDATA[host]]>
  </INFO>
  <INFO key="cvss">
    <![CDATA[all]]>
  </INFO>
  <INFO key="host_details">
    <![CDATA[1]]>
  </INFO>
  <INFO key="host_ag_details">
    <![CDATA[1]]>
  </INFO>
  <INFO key="qualys_system_ids">
    <![CDATA[1]]>
  </INFO>
  <INFO key="include_text_summary">
    <![CDATA[1]]>
```

```
    </INFO>
    <INFO key="include_vuln_details">
      <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_threat">
      <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_impact">
      <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_solution">
      <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_vpatch">
      <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_compliance">
      <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_exploit">
      <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_malware">
      <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_results">
      <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_appendix">
      <![CDATA[0]]>
    </INFO>
    <INFO key="exclude_account_id">
      <![CDATA[0]]>
    </INFO>
    <INFO key="include_vuln_details_reopened">
      <![CDATA[1]]>
    </INFO>
    <INFO key="metadata_ec2_instances">
      <![CDATA[1]]>
    </INFO>
    <INFO key="cloud_provider_metadata">
      <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_detection_logic">
      <![CDATA[1]]>
    </INFO>
    <INFO key="include_trurisk_details">
      <![CDATA[0]]>
    </INFO>
  </DISPLAY>
  <FILTER>
    <INFO key="selective_vulns">
      <![CDATA[complete]]>
    </INFO>
    <INFO key="search_list_ids">
```

```
    <![CDATA[]]>
  </INFO>
  <INFO key="exclude_qid_option">
    <![CDATA[0]]>
  </INFO>
  <INFO key="exclude_search_list_ids">
    <![CDATA[]]>
  </INFO>
  <INFO key="included_os">
    <![CDATA[ALL]]>
  </INFO>
  <INFO key="status_new">
    <![CDATA[1]]>
  </INFO>
  <INFO key="status_active">
    <![CDATA[1]]>
  </INFO>
  <INFO key="status_reopen">
    <![CDATA[1]]>
  </INFO>
  <INFO key="status_fixed">
    <![CDATA[1]]>
  </INFO>
  <INFO key="vuln_active">
    <![CDATA[1]]>
  </INFO>
  <INFO key="vuln_disabled">
    <![CDATA[1]]>
  </INFO>
  <INFO key="vuln_ignored">
    <![CDATA[1]]>
  </INFO>
  <INFO key="potential_active">
    <![CDATA[1]]>
  </INFO>
  <INFO key="potential_disabled">
    <![CDATA[1]]>
  </INFO>
  <INFO key="potential_ignored">
    <![CDATA[1]]>
  </INFO>
  <INFO key="ig_active">
    <![CDATA[1]]>
  </INFO>
  <INFO key="ig_disabled">
    <![CDATA[1]]>
  </INFO>
  <INFO key="ig_ignored">
    <![CDATA[0]]>
  </INFO>
  <INFO key="display_non_running_kernels">
    <![CDATA[0]]>
  </INFO>
  <INFO key="exclude_non_running_kernel">
    <![CDATA[1]]>
```

```
        </INFO>
        <INFO key="exclude_non_running_services">
          <![CDATA[1]]>
        </INFO>
        <INFO key="exclude_superceded_patches">
          <![CDATA[0]]>
        </INFO>
        <INFO key="exclude_qids_not_exploitable_due_to_configuration">
          <![CDATA[0]]>
        </INFO>
        <INFO key="categories_list">
          <![CDATA[ALL]]>
        </INFO>
        <INFO key="qds_score_min">
          <![CDATA[]]>
        </INFO>
        <INFO key="qds_score_max">
          <![CDATA[]]>
        </INFO>
        <INFO key="exclude_kpatch_cve">
          <![CDATA[1]]>
        </INFO>
      </FILTER>
      <SERVICESPORTS>
        <INFO key="required_services">
          <![CDATA[]]>
        </INFO>
        <INFO key="unauthorized_services">
          <![CDATA[]]>
        </INFO>
        <INFO key="services_info">
          <![CDATA[]]>
        </INFO>
        <INFO key="required_ports">
          <![CDATA[]]>
        </INFO>
        <INFO key="unauthorized_ports">
          <![CDATA[]]>
        </INFO>
      </SERVICESPORTS>
      <USERACCESS>
        <INFO key="global">
          <![CDATA[1]]>
        </INFO>
        <INFO key="report_access_users">
          <![CDATA[]]>
        </INFO>
      </USERACCESS>
    </SCANTEMPLATE>
</REPORTTEMPLATE>
```

### Host List Detection API: Support to Display All CVEs and Exclude Live Patched CVEs

| | |
|---|---|
| New or Updated API | Updated |
| API Endpoint | /api/5.0/fo/asset/host/vm/detection/ |
| Method | GET |
| DTD or XSD Changes | Yes |

You can now view all CVEs when you execute this API with the input parameter show_cve set to 1. You can also exclude all CVEs or QIDs that contain the list of all CVEs using the input parameter exclude_patched_cve set to 1. You can gain visibility and control over the vulnerability data to display all CVEs or exclude live patched CVEs. This helps you to make decisions and prioritize remediation effectively.

**Input Parameter:**

| Parameter | Required/ Optional | Data Type | Description |
|---|---|---|---|
| show_cve={0\|1} | Optional | Integer | Specify 1 to display all the CVEs. |
| exclude_patched_cve={0\|1} | Optional | Integer | Specify 1 to exclude all the live patched CVEs or complete QIDs. |

**Sample – Display all the CVEs**

**API Request:**

```
curl --location
'<qualys_base_url>/api/5.0/fo/asset/host/vm/detection/?action=list&show_results=1&include_vuln_type=confirmed&output_format=XML&show_cve=1&exclude_patched_cve=1&ips=10.xxx.xx.xxx%2C10.xxx.xx.xxx' \
--header 'X-Requested-With: curl demo2' \
--header 'Authorization: Bearer <JWT Token>'
```

**API Response:**

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"<qualys_base_url>/api/5.0/fo/asset/host/vm/detection/dtd/output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
  <RESPONSE>
    <DATETIME>2025-10-15T03:58:12Z</DATETIME>
    <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
    <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
    <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
    <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
    <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
    <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
    <HOST_LIST>
      <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
      <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
```

```
        <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
        <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
        <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
        <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
        <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
        <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
        <HOST>
          <ID>16486809</ID>
          <IP>10.xxx.xx.xxx</IP>
          <TRACKING_METHOD>IP</TRACKING_METHOD>
          <NETWORK_ID>0</NETWORK_ID>
          <OS>
            <![CDATA[FreeBSD 2.2.1-4.x / AIX 5.1-5.2]]>
          </OS>
          <OS_CPE>
            <![CDATA[cpe:/o:redhat:enterprise_linux:8.8:::]]>
          </OS_CPE>
          <LAST_SCAN_DATETIME>2025-09-17T05:45:15Z</LAST_SCAN_DATETIME>
          <LAST_VM_SCANNED_DATE>2025-09-02T10:34:34Z</LAST_VM_SCANNED_DATE>
          <LAST_VM_SCANNED_DURATION>1556</LAST_VM_SCANNED_DURATION>
          <LAST_VM_AUTH_SCANNED_DATE>2025-09-
02T10:34:34Z</LAST_VM_AUTH_SCANNED_DATE>

<LAST_VM_AUTH_SCANNED_DURATION>1556</LAST_VM_AUTH_SCANNED_DURATION>
          <DETECTION_LIST>
            <DETECTION>
              <UNIQUE_VULN_ID>200169535</UNIQUE_VULN_ID>
              <QID>70001</QID>
              <TYPE>Confirmed</TYPE>
              <SEVERITY>3</SEVERITY>
              <SSL>0</SSL>
              <RESULTS>
                <![CDATA[Device Name       Comment       Type
print$  Printer Drivers 0
share           0
IPC$    IPC Service (Samba 4.19.4)      -2147483645]]>
              </RESULTS>
              <STATUS>New</STATUS>
              <FIRST_FOUND_DATETIME>2025-09-02T10:34:34Z</FIRST_FOUND_DATETIME>
              <LAST_FOUND_DATETIME>2025-09-02T10:34:34Z</LAST_FOUND_DATETIME>
              <TIMES_FOUND>1</TIMES_FOUND>
              <LAST_TEST_DATETIME>2025-09-02T10:34:34Z</LAST_TEST_DATETIME>
              <LAST_UPDATE_DATETIME>2025-09-17T05:45:14Z</LAST_UPDATE_DATETIME>
              <IS_IGNORED>0</IS_IGNORED>
              <IS_DISABLED>0</IS_DISABLED>
              <LAST_PROCESSED_DATETIME>2025-09-
17T05:45:14Z</LAST_PROCESSED_DATETIME>
            </DETECTION>
            <DETECTION>
              <UNIQUE_VULN_ID>200169501</UNIQUE_VULN_ID>
              <QID>70003</QID>
              <TYPE>Confirmed</TYPE>
              <SEVERITY>4</SEVERITY>
              <SSL>0</SSL>
              <CVE>CVE-1999-0519</CVE>
```

```
                <STATUS>New</STATUS>
                <FIRST_FOUND_DATETIME>2025-09-02T10:34:34Z</FIRST_FOUND_DATETIME>
                <LAST_FOUND_DATETIME>2025-09-02T10:34:34Z</LAST_FOUND_DATETIME>
                <TIMES_FOUND>1</TIMES_FOUND>
                <LAST_TEST_DATETIME>2025-09-02T10:34:34Z</LAST_TEST_DATETIME>
                <LAST_UPDATE_DATETIME>2025-09-17T05:45:14Z</LAST_UPDATE_DATETIME>
                <IS_IGNORED>0</IS_IGNORED>
                <IS_DISABLED>0</IS_DISABLED>
                <LAST_PROCESSED_DATETIME>2025-09-
17T05:45:14Z</LAST_PROCESSED_DATETIME>
            </DETECTION>
            <DETECTION>
                <UNIQUE_VULN_ID>200214793</UNIQUE_VULN_ID>
                <QID>384506</QID>
                <TYPE>Confirmed</TYPE>
                <SEVERITY>3</SEVERITY>
                <SSL>0</SSL>
                <CVE>CVE-2023-48161,CVE-2024-21208,CVE-2024-21210,CVE-2024-21217,CVE-
2024-21235</CVE>
                <RESULTS>
                    <![CDATA[VENDOR PATH INSTALLED_VERSION REQUIRED_VERSION
Red Hat, Inc /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.412.b08-2.el8.x86_64/jre 1.8.0_412 1.8.0_432]]>
                </RESULTS>
                <STATUS>New</STATUS>
                <FIRST_FOUND_DATETIME>2025-09-02T10:34:34Z</FIRST_FOUND_DATETIME>
                <LAST_FOUND_DATETIME>2025-09-02T10:34:34Z</LAST_FOUND_DATETIME>
                <TIMES_FOUND>1</TIMES_FOUND>
                <LAST_TEST_DATETIME>2025-09-02T10:34:34Z</LAST_TEST_DATETIME>
                <LAST_UPDATE_DATETIME>2025-09-22T08:04:57Z</LAST_UPDATE_DATETIME>
                <IS_IGNORED>0</IS_IGNORED>
                <IS_DISABLED>0</IS_DISABLED>
                <LAST_PROCESSED_DATETIME>2025-09-
22T08:04:57Z</LAST_PROCESSED_DATETIME>
            </DETECTION>
…..

          </DETECTION_LIST>
        </HOST>
      </HOST_LIST>
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```


**DTD Output:**


```
<!-- QUALYS HOST_LIST_VM_DETECTION_OUTPUT DTD -->
<!ELEMENT HOST_LIST_VM_DETECTION_OUTPUT (REQUEST?,RESPONSE)>
<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
<!-- if returned, POST_DATA will be urlencoded -->
```

```
<!ELEMENT POST_DATA (#PCDATA)>
<!ELEMENT RESPONSE (DATETIME, HOST_LIST?, WARNING?)>
<!ELEMENT HOST_LIST (HOST+)>
<!ELEMENT HOST (ID, ASSET_ID?, IP?, IPV6?, TRACKING_METHOD?, ASSET_GROUP_LIST?,
NETWORK_ID?, NETWORK_NAME?, OS_HOSTNAME?,
        OS?, OS_CPE?, DNS?, DNS_DATA?, CLOUD_PROVIDER?, CLOUD_SERVICE?,
CLOUD_RESOURCE_ID?, EC2_INSTANCE_ID?, NETBIOS?, QG_HOSTID?,
        LAST_SCAN_DATETIME?, LAST_VM_SCANNED_DATE?,
        LAST_VM_SCANNED_DURATION?, LAST_VM_AUTH_SCANNED_DATE?,
        LAST_VM_AUTH_SCANNED_DURATION?, LAST_PC_SCANNED_DATE?, TAGS?,
METADATA?, CLOUD_PROVIDER_TAGS?, DETECTION_LIST)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT ASSET_ID (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IPV6 (#PCDATA)>
<!ELEMENT TRACKING_METHOD (#PCDATA)>
<!ELEMENT ASSET_GROUP_LIST (EMPTY|ASSET_GROUP)*>
<!ELEMENT ASSET_GROUP (ID, TITLE)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>
<!ELEMENT NETWORK_NAME (#PCDATA)>
<!ELEMENT OS_HOSTNAME (#PCDATA)>
<!ELEMENT OS (#PCDATA)>
<!ELEMENT OS_CPE (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT DNS_DATA (HOSTNAME?, DOMAIN?, FQDN?)>
<!ELEMENT HOSTNAME (#PCDATA)>
<!ELEMENT DOMAIN (#PCDATA)>
<!ELEMENT FQDN (#PCDATA)>
<!ELEMENT CLOUD_PROVIDER (#PCDATA)>
<!ELEMENT CLOUD_SERVICE (#PCDATA)>
<!ELEMENT CLOUD_RESOURCE_ID (#PCDATA)>
<!ELEMENT EC2_INSTANCE_ID (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT QG_HOSTID (#PCDATA)>
<!ELEMENT LAST_SCAN_DATETIME (#PCDATA)>
<!ELEMENT LAST_VM_SCANNED_DATE (#PCDATA)>
<!ELEMENT LAST_VM_SCANNED_DURATION (#PCDATA)>
<!ELEMENT LAST_VM_AUTH_SCANNED_DATE (#PCDATA)>
<!ELEMENT LAST_VM_AUTH_SCANNED_DURATION (#PCDATA)>
<!ELEMENT LAST_PC_SCANNED_DATE (#PCDATA)>
<!ELEMENT TAGS (TAG+)>
<!ELEMENT TAG (TAG_ID?, NAME, COLOR?, BACKGROUND_COLOR?)>
<!ELEMENT TAG_ID (#PCDATA)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT COLOR (#PCDATA)>
<!ELEMENT BACKGROUND_COLOR (#PCDATA)>
<!ELEMENT METADATA (EC2|GOOGLE|AZURE|ALICLOUD)+>
<!ELEMENT EC2 (ATTRIBUTE*)>
<!ELEMENT GOOGLE (ATTRIBUTE*)>
<!ELEMENT AZURE (ATTRIBUTE*)>
<!ELEMENT ALICLOUD (ATTRIBUTE*)>
<!ELEMENT ATTRIBUTE
(NAME,LAST_STATUS,VALUE,LAST_SUCCESS_DATE?,LAST_ERROR_DATE?,LAST_ERROR?)>
<!ELEMENT LAST_STATUS (#PCDATA)>
```

<!ELEMENT LAST_SUCCESS_DATE (#PCDATA)>
<!ELEMENT LAST_ERROR_DATE (#PCDATA)>
<!ELEMENT LAST_ERROR (#PCDATA)>
<!ELEMENT CLOUD_PROVIDER_TAGS (CLOUD_TAG+)>
<!ELEMENT CLOUD_TAG (NAME, VALUE, LAST_SUCCESS_DATE)>
<!ELEMENT DETECTION_LIST (DETECTION+)>
<!ELEMENT DETECTION (UNIQUE_VULN_ID, QID, TYPE, SEVERITY?, PORT?, PROTOCOL?, FQDN?, SSL?, INSTANCE?, RESULT_INSTANCE?,
**CVE?**, RESULTS?, STATUS?,
FIRST_FOUND_DATETIME?, LAST_FOUND_DATETIME?, SOURCE?, VULNERABILITY_DETECTION_SOURCES?, LATEST_VULNERABILITY_DETECTION_SOURCE?,
MITRE_TACTIC_NAME?, MITRE_TECHNIQUE_NAME?, MITRE_TACTIC_ID?, MITRE_TECHNIQUE_ID?, TRURISK_ELIMINATION_STATUS?, QDS?, QDS_FACTORS?, TIMES_FOUND?,
LAST_TEST_DATETIME?,
LAST_UPDATE_DATETIME?,
LAST_FIXED_DATETIME?,
FIRST_REOPENED_DATETIME?, LAST_REOPENED_DATETIME?, TIMES_REOPENED?,
SERVICE?, IS_IGNORED?, IS_DISABLED?, AFFECT_RUNNING_KERNEL?, AFFECT_RUNNING_SERVICE?, AFFECT_EXPLOITABLE_CONFIG?, LAST_PROCESSED_DATETIME?, ASSET_CVE?)>
<!ELEMENT UNIQUE_VULN_ID (#PCDATA)>
<!ELEMENT QID (#PCDATA)>
<!ELEMENT TYPE (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT PROTOCOL (#PCDATA)>
<!ELEMENT SSL (#PCDATA)>
<!ELEMENT INSTANCE (#PCDATA)>
<!ELEMENT RESULT_INSTANCE (#PCDATA)>
**<!ELEMENT CVE (#PCDATA)>**
<!ELEMENT RESULTS (#PCDATA)>
<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT SEVERITY (#PCDATA)>
<!ELEMENT QDS (#PCDATA)>
<!ATTLIST QDS severity CDATA #REQUIRED>
<!ELEMENT QDS_FACTORS (QDS_FACTOR)*>
<!ELEMENT QDS_FACTOR (#PCDATA)>
<!ATTLIST QDS_FACTOR name CDATA #REQUIRED>
<!ELEMENT FIRST_FOUND_DATETIME (#PCDATA)>
<!ELEMENT LAST_FOUND_DATETIME (#PCDATA)>
<!ELEMENT SOURCE (#PCDATA)>
<!ELEMENT VULNERABILITY_DETECTION_SOURCES (#PCDATA)>
<!ELEMENT LATEST_VULNERABILITY_DETECTION_SOURCE (#PCDATA)>
<!ELEMENT MITRE_TACTIC_NAME (#PCDATA)>
<!ELEMENT MITRE_TECHNIQUE_NAME (#PCDATA)>
<!ELEMENT MITRE_TACTIC_ID (#PCDATA)>
<!ELEMENT MITRE_TECHNIQUE_ID (#PCDATA)>
<!ELEMENT TRURISK_ELIMINATION_STATUS (#PCDATA)>
<!ELEMENT TIMES_FOUND (#PCDATA)>
<!ELEMENT LAST_TEST_DATETIME (#PCDATA)>
<!ELEMENT LAST_UPDATE_DATETIME (#PCDATA)>
<!ELEMENT LAST_FIXED_DATETIME (#PCDATA)>
<!ELEMENT FIRST_REOPENED_DATETIME (#PCDATA)>
<!ELEMENT LAST_REOPENED_DATETIME (#PCDATA)>
<!ELEMENT TIMES_REOPENED (#PCDATA)>

```
<!ELEMENT SERVICE (#PCDATA)>
<!ELEMENT IS_IGNORED (#PCDATA)>
<!ELEMENT IS_DISABLED (#PCDATA)>
<!ELEMENT AFFECT_RUNNING_KERNEL (#PCDATA)>
<!ELEMENT AFFECT_RUNNING_SERVICE (#PCDATA)>
<!ELEMENT AFFECT_EXPLOITABLE_CONFIG (#PCDATA)>
<!ELEMENT LAST_PROCESSED_DATETIME (#PCDATA)>
<!ELEMENT ASSET_CVE (#PCDATA)>
<!ELEMENT WARNING (CODE?, TEXT, URL?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!-- EOF -->
```