Qualys Container Security

API Release Notes

Version 1.23

March 08, 2023

Qualys Cloud Suite API gives you many ways to integrate your programs and API calls with Qualys capabilities. You'll find all the details in our user guides, available at the time of release. Just log in to your Qualys account and go to Help > Resources.

What's New

Fetch a Vulnerability Report in JSON Format

End of Life (EOL) for v1.1 and v1.2 Container Security APIs

Qualys API URL

The Qualys API URL you should use for API requests depends on the Qualys platform where your account is located.

Click here to identify your Qualys platform and get the API URL

Fetch a Vulnerability Report in JSON Format

API affected	/csapi/v1.3/reports/jsonReport
Operator	GET
New or Updated APIs	New

We have introduced a new API to fetch vulnerability reports in JSON format. This allows you to use the report data seamlessly in further processes such as automation and integrations.

Note: If you want to maintain audit logs for JSON reporting, you need to record the requests and responses at your end.

Input Parameters

Field Name	Mandatory	Data Type	Description
templateName	Yes	string	Specify whether to generate a vulnerability report for images or containers. The valid values are: CS_IMAGE_VULNERABILITY or CS_CONTAINER_VULNERABILITY.
filter	No	string	Provide a QQL query to limit the report to only certain images or containers. Only the images or containers that match your query are included in the report.
paginationQuery	No	string	Provide a query to filter the next page. You can find the pagination query for the next page in the "nexturl" response header.

Sample

Fetch a vulnerability report for all containers in your account.

API Request:

```
curl -X GET
"<qualys_base_url>/csapi/v1.3/reports/jsonReport?templateName=CS_IMAGE_VU
LNERABILITY%20OR%20CS_CONTAINER_VULNERABILITY"
-H "accept: application/*"
-H "Authorization: Bearer <token>"
```

Response:


```
{
    "data": [
        {
            "uuid": "000061b2-b8be-37ed-9196-dc8bbf372fe1",
            "sha":
"a39b0473439ca693b7f36941ac25ce8a27a74538a29bad17c6638f2f521d6e86",
            "containerId": "a39b0473439c",
            "name": "k8s_calico-kube-controllers_calico-kube-controllers-
7dddfdd6c9-qltv4_calico-system_9793b2c9-58f0-4acc-8ded-8a52b3283d43_111",
            "imageId": "c95ddb97ba59",
            "created": "2022-11-24 06:25:10 +0000 UTC",
            "hostName": "ip-10-82-8-106",
            "hostIp": "10.82.8.106",
            "state": "STOPPED",
            "stateChanged": "2022-11-28 06:41:00 +0000 UTC",
            "lastScanned": "",
            "updated": "2022-11-28 06:41:01 +0000 UTC",
            "hostArchitecture": ["x86_64"
                                ],
            "podName": "",
            "podUuid": "",
            "podNameSpace": "",
            "podLabel": "",
            "podController": "",
            "nodeName": "",
            "nodeIsMaster": "",
            "repository": "",
            "qid": null,
            "title": null,
            "severity": null,
            "category": null,
            "cveids": null,
            "vendorReference": null,
            "cvssBase": null,
            "cvssTemporal": null,
            "cvss3Base": null,
            "cvss3Temporal": null,
            "threat": null,
            "impact": null,
            "solution": null,
            "exploitability": null,
            "associatedMalwares": null,
            "software": null,
            "result": null
        },
        {
            "uuid": "01c85531-614e-3661-afe9-4854159310e6",
```

```
            "sha":
"9adb5c83e17cce411ee6ff2a16e8860436f227048bce1ae3586384e5c13f7f83",
            "containerId": "9adb5c83e17c",
            "name": "k8s_calico-typha_calico-typha-5879f89c49-
lqst4_calico-system_fece47ba-4d8d-457a-aa55-dfcfb892fd1a_24",
            "imageId": "9507cf15077f",
            "created": "2022-11-29 04:59:48 +0000 UTC",
            "hostName": "ip-10-82-10-7",
            "hostIp": "10.82.10.7",
            "state": "STOPPED",
            "stateChanged": "2022-12-12 05:30:08 +0000 UTC",
            "lastScanned": "",
            "updated": "2022-12-12 05:30:14 +0000 UTC",
            "hostArchitecture": [
                "x86_64"
            ],
            "podName": "calico-typha-5879f89c49-lqst4",
            "podUuid": "fece47ba-4d8d-457a-aa55-dfcfb892fd1a",
            "podNameSpace": "calico-system",
           "podLabel": " key:k8s-app value:calico-typha, key:pod-template-
hash value:5879f89c49",
            "podController": " uuid:15ad4899-c983-420a-87a4-cb221ada80ef
name:calico-typha type:Deployment, uuid:89f97929-dfc7-4b74-8678-
aec16e46bebd name:calico-typha-5879f89c49 type:ReplicaSet",
            "nodeName": "ip-10-82-10-7",
            "nodeIsMaster": "true",
            "repository": "",
            "qid": null,
            "title": null,
            "severity": null,
            "category": null,
            "cveids": null,
            "vendorReference": null,
            "cvssBase": null,
            "cvssTemporal": null,
            "cvss3Base": null,
            "cvss3Temporal": null,
            "threat": null,
            "impact": null,
            "solution": null,
            "exploitability": null,
            "associatedMalwares": null,
            "software": null,
            "result": null
        }
    ],
    "resourceType": "Container Vulnerability",
    "count": 2000
}
```

End of Life (EOL) for v1.1 and v1.2 Container Security APIs

The End of Life (EOL) for Container Security API versions 1.1 and 1.2 takes effect starting from Container Security release 1.23. That means all API endpoints containing v1.1 or v1.2 in the API path for containers, images, registries, and sensors will no longer be supported.

It is recommended to use the equivalent v1.3 APIs to perform all of your Container Security operations.

This change was communicated in advance through a notification dated December 07, 2022. For more information, see Qualys Cloud Platform API Deprecation Notice.