Qualys Container Security v1.x

API Release Notes

Version 1.19

September 8, 2022

Qualys Container Security API gives you many ways to integrate your programs and API calls with Qualys capabilities.

What's New

SCA Scanning Now Supported

Qualys API URL

Container Security supports both API server URLs and API gateway URLs for API requests.

The Qualys API server or gateway 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

This documentation uses the API URL for Qualys US Platform 2 (https://gateway.qg2.apps.qualys.com) in sample API requests. If you're on another platform, please replace this URL with the appropriate server URL for your account.

SCA Scanning Now Supported

This release brings support for Software Composition Analysis (SCA) scanning of container images. An SCA scan discovers installed open source software and libraries, as well as associated vulnerabilities, present in your container images.

While evaluating security posture of container images it is important to identify all software packages present in the image. The SCA scan can be used to identify programming language-based software packages inside the image. In addition, metadata information for each image layer is also provided. The SCA scan detects packages for these programming languages: Java, Python, Go, Node.js, .NET.

SCA scanning is supported for all sensor types – General, Registry and CI/CD. It's supported for Docker Runtime only. SCA scanning is only supported when scanning container images. SCA scanning is not supported for Mac OS.

Prerequisites

- The SCA Scanning feature must be enabled for your subscription. Contact Qualys Support to have this feature enabled.
- Update your sensors to version 1.19 or later.
- Relaunch your sensors with the parameter --perform-sca-scan to perform SCA scanning.

How it Works

SCA scanning is not performed by default. Users must enable SCA scanning using the new parameter --perform-sca-scan when deploying their sensors. When enabled, an SCA scan is performed after a standard vulnerability scan (Static or Dynamic) on your container images. When the SCA scan completes, the sensor uploads the metadata information collected by the scan to the Qualys backend where posture evaluation is performed. You can view SCA scan data findings in the Container Security UI and API as part of image details. Vulnerability detections found by the SCA scan are presented as QIDs. Filters are provided so you can identify the type of scan (SCA, Dynamic or Static) used to detect a particular vulnerability.

API Updates

We updated the response for the following Image APIs. When you fetch a list of images, image details or a detailed list of images, the response shows a new field called **scanTypes** where you'll see the type or types of scans run on the image. Values may include SCA, Dynamic and Static. For software packages and vulnerabilities that were detected by an SCA scan, you'll see **scanType: SCA** in the software and vulnerability details.

See API samples in the sections that follow.

Fetch a list of images

Fetch image details

Fetch a detailed list of images

Fetch a list of software installed on an image

Fetch vulnerability details for an image

Fetch a list of images

/v1.3/images

[GET]

API request:

```
curl -X GET
'https://gateway.qg2.apps.qualys.com/csapi/v1.3/images?pageNumber=1&pageS
ize=50&sort=created%3Adesc' --header 'Authorization: Bearer <token>'
```

Response:


```
{
      "created": "1525522580000",
      "updated": "1661479716359",
      "sha":
"0645d07d36305947d72a31282e2dd035f54fbeff6d9adb6701e9c72e75f675e8",
      "repo": [
        {
          "registry": "docker.io",
          "tag": "0.9.2",
          "repository": "known"
        }
      ],
      "repoDigests": [
        {
          "registry": "docker.io",
          "digest":
"a3cfd95b4ff72c4f1f33aa98aae1d86b9ed1bfe050058fb46205540280e9937f",
```

```
      "repository": "known"
    }
  ],
  "uuid": "38aa3900-f803-32a7-9806-39233e66b85c",
  "size": 539069295,
  "vulnerabilities": {
    "severity5Count": 8,
    "severity3Count": 54,
    "severity4Count": 13,
    "severity1Count": 1,
    "severity2Count": 1
  },
  "imageId": "0645d07d3630",
  "associatedContainersCount": 1,
  "associatedHostsCount": 1,
  "lastVmScanDate": "1661479716359",
  "registryUuid": null,
  "source": [
    "GENERAL"
  ],
  "isDockerHubOfficial": false,
  "isInstrumented": false,
  "instrumentedFrom": null,
  "instrumentationState": null,
  "scanType": null,
  "scanTypes": [
    "SCA",
    "DYNAMIC"
  ],
  "scanErrorCode": null,
  "scanStatus": "SUCCESS",
  "lastFoundOnHost": {
    "sensorUuid": "2ed740ac-acba-47b5-8072-aaa739e44f0d",
    "hostname": "ip-10-20-30-40",
    "ipAddress": "10.20.30.40",
    "uuid": "721e3460-bced-4ec0-b695-3c3349eefefb",
    "lastUpdated": "2022-08-26T01:57:22.110Z"
  },
  "compliance": {
    "failCount": 2,
    "passCount": 0,
    "errorCount": 0
  },
  "lastComplianceScanDate": "1661479044741"
}
```

Fetch image details

/v1.3/images/{imageSha}

[GET]

API request:

```
curl -X GET
'https://gateway.qg2.apps.qualys.com/csapi/v1.3/images/0645d07d36305947d7
2a31282e2dd035f54fbeff6d9adb6701e9c72e75f675e8' --header 'Authorization:
Bearer <token>'
```

Response:


```
{
  "created": "1525522580000",
  "updated": "1661479716359",
  "author": "hello@withknown.com",
  "repo": [
    {
      "registry": "docker.io",
      "tag": "0.9.2",
      "repository": "known"
    }
  ],
  "repoDigests": [
    {
      "registry": "docker.io",
      "digest":
"a3cfd95b4ff72c4f1f33aa98aae1d86b9ed1bfe050058fb46205540280e9937f",
      "repository": "known"
    }
  ],
  "label": null,
  "uuid": "38aa3900-f803-32a7-9806-39233e66b85c",
  "sha":
"0645d07d36305947d72a31282e2dd035f54fbeff6d9adb6701e9c72e75f675e8",
  "operatingSystem": "Debian Linux 8.10",
  "customerUuid": "98c16d24-d2c1-53c9-8200-4468190aff46",
  "dockerVersion": "17.06.2-ce",
  "size": 539069295,
  "layers": [
    {
      "size": "126775160",
      "createdBy": "ADD
file:3e6141c0c9cb74b14a281eb3ab7aaf162a625733e652c3948b323bb2ec8b4343 in
/ ",
      "created": "1524897855000",
      "comment": "",
```

```
      "id": null,
      "sha": null,
      "tags": null
    },
    {
      "size": "0",
      "createdBy": "CMD [\"bash\"]",
      "created": "1524897856000",
      "comment": "",
      "id": null,
      "sha": null,
      "tags": null
    },
...
  ],
  "host": [
    {
      "sensorUuid": "2ed740ac-acba-47b5-8072-aaa739e44f0d",
      "hostname": "ip-10-20-30-40",
      "ipAddress": "10.20.30.40",
      "uuid": "721e3460-bced-4ec0-b695-3c3349eefefb",
      "lastUpdated": "2022-08-26T01:57:22.110Z"
    }
  ],
  "hostArchitecture": [
    "x86_64"
  ],
  "architecture": "amd64",
  "imageId": "0645d07d3630",
  "lastScanned": "1661479716359",
  "registryUuid": null,
  "source": [
    "GENERAL"
  ],
  "totalVulCount": "77",
  "users": [
    "root"
  ],
  "isDockerHubOfficial": null,
  "isInstrumented": null,
  "instrumentedFrom": null,
  "instrumentationState": null,
  "scanType": null,
  "scanTypes": [
    "SCA",
    "DYNAMIC"
  ],
  "scanErrorCode": null,
  "scanStatus": "SUCCESS",
```

```
  "lastFoundOnHost": {
    "sensorUuid": "2ed740ac-acba-47b5-8072-aaa739e44f0d",
    "hostname": "ip-10-20-30-40",
    "ipAddress": "10.20.30.40",
    "uuid": "721e3460-bced-4ec0-b695-3c3349eefefb",
    "lastUpdated": "2022-08-26T01:57:22.110Z"
  },
...
```


Fetch a detailed list of images

/v1.3/images/list

[GET]

API request:

```
curl -X GET
'https://gateway.qg2.apps.qualys.com/csapi/v1.3/images/list?limit=2' --
header 'Authorization: Bearer <token>'
```

Response:


```
{
  "data": [
    {
      "created": "1660094821000",
      "updated": "1661479235359",
      "author": "",
      "repo": [
        {
          "registry": "docker.io",
          "tag": "latest",
          "repository": "vault"
        }
      ],
      "repoDigests": [
        {
          "registry": "docker.io",
          "digest":
"f2c0f82d1bde88a6608f26468258306e48ac46a4d353db2151e26e0fd00928bb",
          "repository": "vault"
        }
      ],
      "label": null,
      "uuid": "a449db68-b539-33f1-8bc0-723c9e9c6e0a",
      "sha":
"22fdc6314051df714eb280680c24524ed01d0ed2eddff1358cc40d528c82579e",
      "operatingSystem": "Alpine Linux 3.14.8",
```

```
      "customerUuid": "98c16d24-d2c1-53c9-8200-4468190aff46",
      "dockerVersion": "20.10.12",
      "size": 207222566,
      "layers": [
         {
          "size": "0",
          "createdBy": "CMD [\"/bin/sh\"]",
          "created": "1660065608000",
          "comment": "",
          "id": null,
          "sha": null,
          "tags": null
        },
...
      "architecture": "amd64",
      "imageId": "22fdc6314051",
      "lastScanned": "1661479235359",
      "registryUuid": null,
      "source": [
        "GENERAL"
      ],
      "users": [
        "root"
      ],
      "lastFoundOnHost": {
        "sensorUuid": "2ed740ac-acba-47b5-8072-aaa739e44f0d",
        "hostname": "ip-10-20-30-40",
        "ipAddress": "10.20.30.40",
        "uuid": "721e3460-bced-4ec0-b695-3c3349eefefb",
        "lastUpdated": "2022-08-26T01:57:22.110Z"
      },
      "isDockerHubOfficial": null,
      "isInstrumented": null,
      "instrumentedFrom": null,
      "instrumentationState": null,
      "scanType": null,
      "scanTypes": [
        "DYNAMIC",
        "SCA"
      ],
      "softwares": [
        {
          "name": "github.com/hashicorp/golang-lru",
          "version": "v0.5.4",
          "fixVersion": null,
          "scanType": "SCA",
          "packagePath": "bin/vault"
        },
        {
```

```
          "name": "github.com/xdg-go/scram",
          "version": "v1.0.2",
          "fixVersion": null,
          "scanType": "SCA",
          "packagePath": "bin/vault"
        },
        {
          "name": "github.com/coreos/go-systemd/v22",
          "version": "v22.3.2",
          "fixVersion": null,
          "scanType": "SCA",
          "packagePath": "bin/vault"
        },
        {
          "name": "libxcrypt",
          "version": "4.1.1-6.el8",
          "fixVersion": null,
          "scanType": "DYNAMIC",
          "packagePath": null
        },
...
      "vulnerabilities": [
        {
          "qid": 980408,
          "result": "#table cols=\"5\"\nPackage Installed_Version
Required_Version Language Install_Path\norg.jsoup:jsoup 1.12.1 1.14.2
Java usr/share/maven/lib/wagon-http-3.4.3-shaded.jar",
          "software": [
            {
              "name": "org.jsoup:jsoup",
              "version": "1.12.1",
              "fixVersion": "1.14.2",
              "scanType": "SCA",
              "packagePath": "usr/share/maven/lib/wagon-http-3.4.3-
shaded.jar"
            }
          ],
          "lastFound": "1661479693756",
          "firstFound": "1661479693756",
          "typeDetected": "CONFIRMED",
          "scanType": [
            "SCA"
          ]
        },
        {
          "qid": 980276,
          "result": "#table cols=\"5\"\nPackage Installed_Version
Required_Version Language Install_Path\ncom.google.guava:guava 25.1-
android 30.0-jre Java usr/share/maven/lib/guava-25.1-android.jar",
```

```
          "software": [
            {
              "name": "com.google.guava:guava",
              "version": "25.1-android",
              "fixVersion": "30.0-jre",
              "scanType": "SCA",
              "packagePath": "usr/share/maven/lib/guava-25.1-android.jar"
            }
          ],
          "lastFound": "1661479693755",
          "firstFound": "1661479693755",
          "typeDetected": "CONFIRMED",
          "scanType": [
            "SCA"
          ]
        },
        {
          "qid": 159808,
          "result": "#table cols=\"3\"\nPackage Installed_Version
Required_Version\nplatform-python 3.6.8-41.0.1.el8.x86__64 3.6.8-
45.0.1.el8\npython3-libs 3.6.8-41.0.1.el8.x86__64 3.6.8-45.0.1.el8",
          "software": [
            {
              "name": "platform-python",
              "version": "3.6.8-41.0.1.el8",
              "fixVersion": "3.6.8-45.0.1.el8",
              "scanType": "DYNAMIC",
              "packagePath": null
            },
            {
              "name": "python3-libs",
              "version": "3.6.8-41.0.1.el8",
              "fixVersion": "3.6.8-45.0.1.el8",
              "scanType": "DYNAMIC",
              "packagePath": null
            }
          ],
          "lastFound": "1661479693755",
          "firstFound": "1661479693755",
          "typeDetected": "CONFIRMED",
          "scanType": [
            "DYNAMIC"
          ]
        },
 ...
```

Fetch a list of software installed on an image

/v1.3/images/{imageId}/software

[GET]

API request:

```
curl -X GET
'https://gateway.qg2.apps.qualys.com/csapi/v1.3/images/5d556c82899c/softw
are' --header 'Authorization: Bearer <token>'
```

Response:

```
{
  "data": [
    {
      "name": "libpsl",
      "version": "0.20.2-6.el8",
      "scanType": "DYNAMIC",
      "packagePath": null,
      "fixVersion": null,
      "vulnerabilities": {
        "severity5Count": null,
        "severity4Count": null,
        "severity3Count": null,
        "severity2Count": null,
        "severity1Count": null
      }
    },
      },
    {
      "name": "org.apache.maven.resolver:maven-resolver-transport-wagon",
      "version": "1.6.3",
      "scanType": "SCA",
      "packagePath": "usr/share/maven/lib/maven-resolver-transport-wagon-
1.6.3.jar",
      "fixVersion": null,
      "vulnerabilities": {
        "severity5Count": null,
        "severity4Count": null,
        "severity3Count": null,
        "severity2Count": null,
        "severity1Count": null
      }
    },
...
```

Fetch vulnerability details for an image

/v1.3/images/{imageId}/vuln

[GET]

API request:

```
curl -X GET
'https://gateway.qg2.apps.qualys.com/csapi/v1.3/images/5d556c82899c/vuln?
type=ALL&sort=qid%3Aasc' --header 'Authorization: Bearer <token>'
```

Response:


```
{
  "details": [
    {
      "vulnerability": null,
      "result": "#table cols=\"3\"\nPackage Installed_Version
Required_Version\nopenssl-libs 1.1.1k-4.el8.x86__64 1.1.1k-7.el8__6",
      "lastFound": "1661479693755",
      "firstFound": "1661479693755",
      "severity": 5,
      "customerSeverity": 5,
      "port": null,
      "typeDetected": "CONFIRMED",
      "status": null,
      "risk": 50,
      "category": "OEL",
      "discoveryType": [
        "AUTHENTICATED"
      ],
      "authType": [
        "UNIX_AUTH"
      ],
      "supportedBy": [
        "VM",
        "CA-Linux Agent"
      ],
      "product": [
        "openssl"
      ],
      "vendor": [
        "oracle"
      ],
      "cveids": [
        "CVE-2022-2097",
        "CVE-2022-1292",
        "CVE-2022-2068"
      ],
```

```
      "threatIntel": {
        "activeAttacks": null,
        "zeroDay": null,
        "publicExploit": null,
        "highLateralMovement": true,
        "easyExploit": true,
        "highDataLoss": true,
        "noPatch": null,
        "denialOfService": true,
        "malware": null,
        "exploitKit": null,
        "publicExploitNames": null,
        "malwareNames": null,
        "exploitKitNames": null
      },
      "qid": 980351,
      "title": "Java (maven) Security Update for commons-io:commons-io
(GHSA-gwrp-pvrq-jmwv)",
      "cvssInfo": {
        "baseScore": "5.8",
        "temporalScore": "4.3",
        "accessVector": "Network"
      },
      "cvss3Info": {
        "baseScore": "4.8",
        "temporalScore": "4.2"
      },
      "patchAvailable": true,
      "published": 1647355370000,
      "scanType": [
        "SCA"
      ],
      "software": [
        {
          "name": "commons-io:commons-io",
          "version": "2.6",
          "scanType": "SCA",
          "packagePath": "usr/share/maven/lib/wagon-http-3.4.3-
shaded.jar",
          "fixVersion": "2.7",
          "vulnerabilities": null
        }
      ]
    },
...
```