Qualys Container Security v1.x

API Release Notes

Version 1.3

July 26, 2018

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

What's New

Fetch CVSS scores and list of vulnerable software

List privileged containers

URL to the Qualys API Server

Qualys maintains multiple Qualys platforms. The Qualys API server URL that you should use for API requests depends on the platform where your account is located.

Account Location	Platform URL
Qualys US Platform 1	https://qualysguard.qualys.com
Qualys US Platform 2	https://qualysguard.qg2.apps.qualys.com
Qualys US Platform 3	https://qualysguard.qg3.apps.qualys.com
Qualys EU Platform 1	https://qualysguard.qualys.eu
Qualys EU Platform 2	https://qualysapi.qg2.apps.qualys.eu
Qualys India Platform 1	https://qualysguard.qg1.apps.qualys.in

Fetch CVSS scores and list of vulnerable software

API affected	/csapi/v1.1/containers
New or Updated APIs	Updated

The containers API now fetches information on:

- CVSS and CVSS3 info with base and temporal scores

- Vulnerable software with fixed version and related QIDs

Sample

Here's sample request and output to get the CVSS and vulnerable software information for a container.

API request:

```
curl -X GET --header 'Accept: application/json' --header 'Authorization:
Basic cXVheXNfYmczOnFhdGVtcEAxMjM='
'https://<QualysURL>/csapi/v1.1/containers/c4905cc26d35/vuln?filter=not%2
0software%20is%20null&type=ALL&isRogue=false'
```

Response:


```
{
  "details": {
    "vulns": [
      {
        "vulnerability": null,
        "result": "gpgv 2.1.18-8~deb9u1 2.1.18-8~deb9u2",
        "lastFound": "1531310274031",
        "firstFound": "1529489657816",
        "fixed": null,
        "severity": 3,
        "customerSeverity": 3,
        "port": null,
        "typeDetected": "CONFIRMED",
        "status": null,
        "nonRunningKernel": null,
        "nonExploitableConfig": null,
        "runningService": null,
        "risk": 30,
        "category": "Debian",
        "os": null,
        "discoveryType": [
          "AUTHENTICATED"
        ],
        "authType": [
```

```
    "UNIX_AUTH"
  ],
  "supportedBy": [
    "VM",
    "CA-Linux Agent"
  ],
  "product": [
    "None"
  ],
  "vendor": [
    "debian"
  ],
  "cveids": [
    "CVE-2018-12020"
  ],
  "threatIntel": {
    "activeAttacks": null,
    "zeroDay": null,
    "publicExploit": null,
    "highLateralMovement": null,
    "easyExploit": null,
    "highDataLoss": null,
    "noPatch": null,
    "denialOfService": null,
    "malware": null,
    "exploitKit": null,
    "publicExploitNames": null,
    "malwareNames": null,
    "exploitKitNames": null
  },
  "qid": 176405,
  "title": "Debian Security Update for gnupg2 (DSA 4222-1)",
  "cvssInfo": {
    "baseScore": "6.0",
    "temporalScore": "4.4",
    "accessVector": "Network"
  },
  "cvss3Info": {
    "baseScore": "5.0",
    "temporalScore": "4.4"
  },
  "patchAvailable": true,
  "software": [
    {
      "name": "gpgv",
      "version": "2.1.18-8~deb9u1",
      "fixVersion": "2.1.18-8~deb9u2",
      "vulnerabilities": null
    }
```

```
      ]
    }
  ],
  "rougeVulns": null
},
"vulnSummary": {
  "confirmed": {
    "sev1Count": 0,
    "sev5Count": 0,
    "sev2Count": 1,
    "sev4Count": 0,
    "sev3Count": 2
  },
  "potential": {
    "sev1Count": 0,
    "sev5Count": 0,
    "sev2Count": 1,
    "sev4Count": 0,
    "sev3Count": 2
  },
  "patchAvailability": {
    "confirmed": {
      "sev1Count": 0,
      "sev5Count": 0,
      "sev2Count": 0,
      "sev4Count": 0,
      "sev3Count": 2
    },
    "potential": {
      "sev1Count": 0,
      "sev5Count": 0,
      "sev2Count": 0,
      "sev4Count": 0,
      "sev3Count": 2
    }
```

List privileged containers

API affected	/csapi/v1.1/containers
New or Updated APIs	Updated

The containers API now fetches privileged containers.

Sample

Here's sample request and output to fetch a list of privileged containers in your account.

API request:

```
curl -X GET --header 'Accept: application/json' --header 'Authorization:
Basic cXVheXNfYmczOnFhdGVtcEAxMjM='
'https://<QualysURL>/csapi/v1.1/containers?filter=privileged%20%3A%20true
&pageNo=0&pageSize=50&sort=created%3Adesc'
```

Response:


```
{
  "data": [
    {
      "imageId": "113a43faa138",
      "created": "1530078190000",
      "uuid": "c0e1da84-fb40-3543-92e4-c3d0f48eec4e",
      "name": "container_new",
      "host": {
        "sensorUuid": "9a40cc0f-4b6e-436d-bacf-a58c337d627b",
        "hostname": "qubu1604ltsssdp4",
        "ipAddress": "10.11.62.176",
        "uuid": "878b906c-9382-48dd-8d68-d4768db5c801",
        "runningContainerCount": null,
        "stoppedContainerCount": null,
        "runningImageContainerCount": null,
        "stoppedImageContainerCount": null
      },
      "state": "DELETED",
      "imageUuid": "bc8ce5b5-1f0f-35f0-b26c-a2589a80c291",
      "containerId": "993a82c8d9d1",
      "stateChanged": "1530078465185",
      "lastScanned": null,
      "vulnerabilities": {
        "severity5Count": 0,
        "severity3Count": 0,
        "severity4Count": 0,
        "severity1Count": 0,
        "severity2Count": 0
```

```
      },
      "rogueVulnerabilities": null,
      "rogueSoftware": null,
      "softwareCount": null
    }
  ],
  "count": 1,
  "groups": {}
}
```