Qualys Container Security

API Release Notes

Version 1.27

July 25, 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

Improved Vulnerability Reports

Vulnerability Exception Management

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

Improved Vulnerability Reports

With this release, you can add the following new columns to image and container vulnerability reports to show details about Qualys tags and Real-time Threat Indicators (RTIs) associated with the image or container:

Parameter	Newly Supported Values	Column Name in the Report
displayColumns	tags	Tags
	easyExploit	Easy Exploit
	noPatch	No Patch
	activeAttacks	Active Attacks
	highLateralMovement	High Lateral Movement
	highDataLoss	High Data Loss
	denialOfService	Denial of Service

For information about these RTIs, see in the Knowledgebase: Real-time Threat Indicators.

The following APIs are impacted:

- Create a Report Request
- Fetch a List of Reports
- Create a Report Schedule

Create a Report Request

API affected	/csapi/v1.3/reports
Operator	POST
New or Updated APIs	Updated
DTD or XSD Changes	NA

You can now show the new columns for tags and RTIs in the report.

Input Parameters

Parameter	New Values	Data Type	Description
displayColumns	tags easyExploit noPatch activeAttacks highLateralMovement highDataLoss denialOfService	string	Include columns for Qualys tags and RTIs associated with the image or container.

Sample: Create a Report with RTI Information

API Request:

```
curl -X POST
"<qualys_base_url>/csapi/v1.3/reports"
-d "{"description":"Demo Report","name":"My Container
Report","templateName":"CS_CONTAINER_VULNERABILITY",
"filter":"status:running","displayColumns":"["containerid","uuid","qid","
tags","easyExploit","noPatch","activeAttacks","highLateralMovement","high
DataLoss","denialOfService"]"}"
--header "Authorization: Bearer <token>"
```

Response:

```
response code 200
{
    "reportUuId": "037570f0-0193-11ea-9327-8fbbd2104c9c"
}
```

Fetch a List of Reports

API affected	/csapi/v1.3/reports
Operator	GET
New or Updated APIs	Updated
DTD or XSD Changes	NA

You can now see the new columns for tags and RTIs in the "displayColumns" output parameter.

Sample: Fetch a List of Reports

API Request:

```
curl -X GET
"<qualys_base_url>/csapi/v1.3/reports?pageNumber=1&pageSize=50" --header
"Authorization: Bearer <token>"
```

Response:

```
{
    "data": [
        {
            "reportUuid": "42699db0-9eb1-11eb-bbb6-833197dc0c5b",
            "createdAt": "2021-04-16T12:42:52.000Z",
            "reportName": "sample-container-report",
            "description": null,
            "fileFormat": "csv",
            "templateName": "CS_CONTAINER_VULNERABILITY",
            "status": "COMPLETED",
            "reportType": "ON_DEMAND",
            "filter": "",
            "displayColumns": [
                "name",
                "containerId",
                "imageId",
                "qid",
                "cveids"
                "tags"
                "easyExploit"
                "noPatch"
                "activeAttacks"
                "highLateralMovement"
                "highDataLoss"
                "denialOfService"
            ]
```

```
        }
        {
            "reportUuid": "4738d060-5b02-11eb-a819-9b3f1886eb36",
            "createdAt": "2021-01-20T09:31:27.000Z",
            "reportName": "sample-image-report",
            "description": null,
            "fileFormat": "csv",
            "templateName": "CS_IMAGE_VULNERABILITY",
            "status": "FAILED",
            "reportType": "ON_DEMAND",
            "filter": null,
            "displayColumns": [
                "ALL"
            ]
        },
    ],
    "count": 2
}
```

Create a Report Schedule

API affected	/csapi/v1.3/reports/schedule
Operator	POST
New or Updated APIs	Updated
DTD or XSD Changes	NA

You can now show the new columns for tags and RTIs in the report.

Sample: Create a Scheduled Report

API Request:

```
curl -X POST
"<qualys_base_url>/csapi/v1.3/reports/schedule/"
-H "accept: application/*"
-H "Authorization: Bearer <token>"
```

Request Body:

```
{
  "name": "CRS-TEST-15",
  "description": "",
  "templateName": "CS_IMAGE_VULNERABILITY",
  "format": "csv",
  "reportScheduleDetails": {
    "recurrenceType": "DAILY",
    "selectedDayOfWeeks": null,
    "monthlyType": null,
    "ordinalDayOfMonth": null,
    "dayOfWeek": null,
    "ordinalDayOfWeek": null
  },
  "displayColumns": [
    "name",
    "containerId",
    "imageId",
    "qid",
    "cveids"
    "tags"
    "easyExploit"
    "noPatch"
    "activeAttacks"
    "highLateralMovement"
    "highDataLoss"
    "denialOfService"
```

```
            ]
  "eventEndTime": "2023-03-25T22:30:00Z",
  "action": "CREATE",
  "eventTime": "2023-02-16T19:30:00Z"
}
```

Request Body:

```
{
  "reportUuid": "620a2490-c3cc-11ed-bf38-5563a478dc98"
}
```

Vulnerability Exception Management

Vulnerability exceptions refer to specific vulnerabilities that have been identified within a containerized environment but are intentionally exempted from remediation measures.

With this release, you can flag the required vulnerabilities as exceptions for specific images. This means that despite their identification, they are intentionally left unreported and unaddressed.

Here are a few possible reasons for granting exceptions:

- **False Positives**: Some vulnerabilities reported may be false positives.

- **Third-Party Dependencies**: Certain vulnerabilities may exist in third-party libraries or components that are beyond your immediate control.

- **Compatibility Issues**: Applying a fix for a vulnerability might have other impacts.

The following new APIs have been introduced for vulnerability exception management:

APIs for Managing the Lists of Vulnerabilities	APIs for Managing the Lists of Vulnerabilities
Create a List	Create a Vulnerability Exception
Update a List	Update a Vulnerability Exception
Show Lists in Your Account	Fetch a List of Vulnerability Exceptions
Fetch Details of a List	Fetch Details of a Vulnerability Exception
Delete a List	Delete an Exception
Fetch Vulnerabilities Associated with a List	Fetch Exceptions Associated with an Image
Update Vulnerabilities Associated with a List	Update Exceptions Associated with an Image
Fetch Vulnerabilities Associated with a List - Bulk API	Fetch Exceptions Associated with a Container
	Update Exceptions Associated with a Container

The following APIs are updated:

- List Images

- Fetch Image Details

- List Containers

- Fetch Container Details

The vulnerabilities or the count of vulnerabilities fetched in the response of the following APIs depends upon the exceptions created for the image or container:

- Fetch Vulnerability Details for an Image *(/v1.3/images/{imageSha}/vuln)*

- Fetch Vulnerability Count for an Image *(/v1.3/images/{imageSha}/vuln/count)*

- Fetch Vulnerability Count for a Container *(/v1.3/containers/{containerSha}/vuln)*

- Fetch Vulnerability Count for a Container *(/v1.3/containers/{containerSha}/vuln/count)*

Create a List

API affected	/csapi/v1.3/list
Operator	POST
New or Updated APIs	New
DTD or XSD Changes	NA

Creates a static list of QIDs to use for creating exceptions.

Input Parameters

Parameter	Mandatory	Data Type	Description
name	Yes	string	Specify a name for the list.
listType	Yes	string	Specify the type of list. Currently, the only valid value is STATIC.
scope	Yes	string	Specify the scope of the list. Currently, the only valid value is VULNERABILITY.
qidsToBeAdded	Yes	string	Specify the QIDs to be added to the list. If the QIDs are specified, the "qidsAdditionFilter" parameter is ignored.
qidsAdditionFilter	Yes	string	Specify a filter query to select QIDs.

Sample: Create a New List of QIDs

API Request:

```
curl -X 'POST'
  '<qualys_base_url>/csapi/v1.3/list'
  -H 'accept: application/json'
  -H 'Authorization: Bearer <token>'
  -H 'Content-Type: application/json'
  -d '{
  "name": "test002_list",
  "listType": "STATIC",
  "scope": "VULNERABILITY",
  "qidsToBeAdded": [
    993395,
    754102,
    92012
  ],
"qidsAdditionFilter": null;
```

```
}'
```

Response:

```
{
  "listUuid": "43bcefbf-74cd-4d67-9b87-f3f4284d8cce"
}
```

Update a List

API affected	/csapi/v1.3/list/{listId}
Operator	PUT
New or Updated APIs	New
DTD or XSD Changes	NA

Updates a static list of QIDs.

Input Parameters

Parameter	Mandatory	Data Type	Description
listId	Mandatory	string	Specify the ID/UUID of the list you want to update.
name	Mandatory	string	Specify a name for the list.
listType	Mandatory	string	Specify the type of list. Currently, the only valid value is STATIC.
scope	Mandatory	string	Specify the scope of the list. Currently, the only valid value is VULNERABILITY.
qidsToBeAdded	Mandatory	string	Specify the QIDs to be added to the list. If the QIDs are specified, the "qidsAdditionFilter" parameter is ignored.
qidsAdditionFilter	Mandatory	string	Specify a filter query to select QIDs. If not required, specify null.

Sample: Update a List of QIDs

API Request:

```
curl -X 'POST'
  '<qualys_base_url>/csapi/v1.3/list'
  -H 'accept: application/json'
  -H 'Authorization: Bearer <token>'
  -H 'Content-Type: application/json'
  -d '{
  "name": "test002_list",
  "listType": "STATIC",
  "scope": "VULNERABILITY",
  "qidsToBeAdded": [
    993395,
    754102,
```

```
      92012
    ],
    "qidsAdditionFilter": null
}'
```

Response:

```
{
  "listUuid": "43bcefbf-74cd-4d67-9b87-f3f4284d8cce"
}
```

Show Lists in Your Account

API affected	/csapi/v1.3/list
Operator	GET
New or Updated APIs	New
DTD or XSD Changes	NA

Fetches the QID lists available in your account.

Input Parameters

Parameter	Mandatory?	Data Type	Description
filter	Optional	string	Filter the lists by providing a query using Qualys syntax. Refer to the "How to Search" topic in the online help for assistance with creating your query.
pageNumber	Optional	integer	The page to be returned. Page numbers start with 1. The default value is 1.
pageSize	Optional	integer	The number of records per page to be included in the response. The default value is 50.
sort	Optional	string	Sort the results using a Qualys token. The default value is status:desc. Refer to the "Sortable tokens" topic in the online help for more information.

Sample: Fetch the Lists from Your Account

API Request:

```
curl -X 'GET'
'<qulays_base_url>/csapi/v1.3/list?pageNumber=1&pageSize=10&sort=status%3
Adesc'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
```

Response:

```
{
```

```
  "data": [
        {
      "listId": "64b2b343-6d3c-43ba-8912-97e45de0b460",
      "name": "Test02_okay",
      "created": "1687518584185",
      "createdBy": "rq30",
      "updated": "1687518584185",
      "updatedBy": "rq30",
      "scope": "VULNERABILITY",
      "listType": "STATIC",
      "qidCount": 52
    },
    {
      "listId": "7788d038-521f-4cc8-9927-eb9b2a87ece4",
      "name": "rails_exc",
      "created": "1687513890947",
      "createdBy": "rq30",
      "updated": "1687513890947",
      "updatedBy": "rq30",
      "scope": "VULNERABILITY",
      "listType": "STATIC",
      "qidCount": 1
    },
    {
      "listId": "43bcefbf-74cd-4d67-9b87-f3f4284d8cce",
      "name": "test002_list",
      "created": "1687752546527",
      "createdBy": "rq30",
      "updated": "1687752546527",
      "updatedBy": "rq30",
      "scope": "VULNERABILITY",
      "listType": "STATIC",
      "qidCount": 0
    },
  ],
  "count": 3
}
```

Show Details of a List

API affected	/csapi/v1.3/list/{listId}
Operator	GET
New or Updated APIs	New
DTD or XSD Changes	NA

Shows details of a QID list.

Input Parameter

Parameter	Mandatory	Data Type	Description
listId	Yes	string	Specify the ID or UUID of the list of which you want to fetch details.

Sample: Fetch Details of a List

API Request:

```
curl -X 'GET' \
'<qualys_base_url>/csapi/v1.3/list/43bcefbf-74cd-4d67-9b87-f3f4284d8cce'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
```

Response:


```
{
  "listId": "43bcefbf-74cd-4d67-9b87-f3f4284d8cce",
  "name": "test002_list",
  "created": "1687752546527",
  "createdBy": "quays_rq30",
  "updated": "1687752546527",
  "updatedBy": "rq30",
  "scope": "VULNERABILITY",
  "listType": "STATIC",
  "qidCount": 3
}
```

Delete a List

API affected	/csapi/v1.3/list/{listId}
Operator	DELETE
New or Updated APIs	New
DTD or XSD Changes	NA

Deletes a QID list from your account.

Note: You cannot delete a list associated with an exception.

Input Parameter

Parameter	Mandatory	Data Type	Description
listId	Yes	string	Specify the ID or UUID of the list you want to delete.

Sample: Delete a List

API Request:

```
curl -X 'DELETE' \
'<qualys_base_url>/csapi/v1.3/list/43bcefbf-74cd-4d67-9b87-f3f4284d8cce'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
```

Response:

```
Response code 200
```

Fetch Vulnerabilities Associated with a List

API affected	/csapi/v1.3/list/{listId}/vulns
Operator	GET
New or Updated APIs	New
DTD or XSD Changes	NA

Fetches vulnerabilities associated with a list.

Input Parameters

Parameter	Mandatory?	Data Type	Description
listId	Mandatory	string	Specify the ID or UUID of the list.
filter	Optional	string	Filter vulnerabilities by providing a query using Qualys syntax. Refer to the "How to Search" topic in the online help for assistance with creating your query.
pageNumber	Optional	integer	The page to be returned. Page numbers start with 1. The default value is 1.
pageSize	Optional	integer	The number of records per page to be included in the response. The default value is 50.
sort	Optional	string	Sort the results using a Qualys token. Refer to the "Sortable tokens" topic in the online help for more information.

Sample: Fetch Vulnerabilities Associated with a List

API Request:

```
curl -X 'GET'
'<qualys_base_url>/csapi/v1.3/list/64b2b343-6d3c-43ba-8912-
97e45de0b460/vulns'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
```

Response:

```
{
    "data": [
        {
            "description": {
              "en": "Suse has released security update for mozillafirefox
to fix the vulnerabilities.<P>Affected Products:<BR> openSUSE Leap
42.2<BR> openSUSE Leap 42.1<BR> openSUSE 13.2<BR> "
            },
            "consequence": {
                "en": "Successful exploitation allows attacker to
compromise the system."
            },
            "solution": {
                "en": "Upgrade to the latest packages which contain a
patch. To install this SUSE Security Update use YaST online_update.
Alternatively you can run the command listed for your product.\n<P>\nTo
install packages using the command line interface, use the command
&amp;quot;yum update&amp;quot;.\n<P>\nRefer to Suse security advisory <A
HREF=\"http://lists.opensuse.org/opensuse-updates/2016-12/msg00020.html\"
TARGET=\"_blank\">openSUSE-SU-2016:2994-1</A> to address this issue and
obtain further details."
            },
            "os": null,
            "discoveryTypes": [
                "AUTHENTICATED"
            ],
            "published": "1486381417000",
            "updated": "1687457302000",
            "types": [
                "VULNERABILITY"
            ],
            "severity": 4,
            "risk": 40,
            "flags": [
                "UNIX_AUTH",
                "PCI_RELATED"
            ],
            "category": "SUSE",
            "authTypes": [
                "UNIX_AUTH"
            ],
            "patches": [
                634478
            ],
            "qid": 169550,
            "exploitability": null,
            "exploits": [
                {
                    "name": "Firefox SVG Animation Remote Code Execution
```

```
Exploit - Core Security Category : Exploits/Client Side",
                    "insertDate": "1483641145000",
                    "firstSeen": null,
                    "link": null,
                    "reference": "CVE-2016-9079",
                    "vendor": {
                        "name": "Core Security",
                        "link": "http://www.coresecurity.com"
                    }
                },
                {
                    "name": "Firefox
nsSMILTimeContainer::NotifyTimeChange() RCE - Metasploit Ref :
/modules/exploit/windows/browser/firefox_smil_uaf",
                    "insertDate": "1485252459000",
                    "firstSeen": "1480464000000",
                    "link": "https://github.com/rapid7/metasploit-
framework/blob/master//modules/exploits/windows/browser/firefox_smil_uaf.
rb",
                    "reference": "CVE-2016-9079",
                    "vendor": {
                        "name": "Metasploit",
                        "link": "http://www.metasploit.com"
                    }
                }
                ...
            ],
            "threatIntel": {
                "activeAttacks": true,
                "zeroDay": null,
                "publicExploit": true,
                "highLateralMovement": null,
                "easyExploit": null,
                "highDataLoss": null,
                "noPatch": null,
                "denialOfService": null,
                "malware": true,
                "exploitKit": null,
                "publicExploitNames": [
                   "Firefox SVG Animation Remote Code Execution Exploit -
Core Security Category : Exploits/Client Side",
                    "Firefox nsSMILTimeContainer::NotifyTimeChange() RCE -
Metasploit Ref : /modules/exploit/windows/browser/firefox_smil_uaf",
                     "Mozilla Firefox < 50.0.2 -
'nsSMILTimeContainer::NotifyTimeChange()' Remote Code Execution
(Metasploit) - The Exploit-DB Ref : 41151",
                  "Firefox 50.0.1 - ASM.JS JIT-Spray Remote Code Execution
- The Exploit-DB Ref : 42327"
                ],
```

```
        "malwareNames": [
            "ShellCode",
            "WebShell",
            "Cryxos",
            "CVE-2019-8039",
            "CVE-2016-9079",
            "ISqrlFX",
            "Pdfka",
            "CVE-2004-0636",
            "CVE-2019-8038",
            "Heuristic",
            "Pdfjsc",
            "Blacole"
        ],
        "exploitKitNames": []
    },
    "malwares": [
        {
            "aliases": null,
            "name": "ShellCode",
            "damage": null,
            "distribution": null,
            "infections": null,
            "link": null,
            "platform": "Script",
            "rating": null,
            "type": "Trojan",
            "firstSeen": "1488423480000",
            "vendor": {
                "name": "ReversingLabs",
                "link": "https://www.reversinglabs.com"
            }
        },
        {
            "aliases": null,
            "name": "WebShell",
            "damage": null,
            "distribution": null,
            "infections": null,
            "link": null,
            "platform": "Script",
            "rating": null,
            "type": "Trojan",
            "firstSeen": "1524585540000",
            "vendor": {
                "name": "ReversingLabs",
                "link": "https://www.reversinglabs.com"
            }
        }
```

```
            ...
        ],
        "title": "OpenSuSE Security Update for MozillaFirefox
(openSUSE-SU-2016:2994-1)",
        "patchAvailable": true,
        "cveIds": [
            "CVE-2016-9078",
            "CVE-2016-9079"
        ],
        "vendorRefs": [
            "openSUSE-SU-2016:2994-1"
        ],
        "bugTraqIds": [
            "94569",
            "94591"
        ],
        "cvssInfo": {
            "baseScore": "6.8",
            "temporalScore": "5.6",
            "accessVector": "Network"
        },
        "cvss3Info": {
            "baseScore": "8.8",
            "temporalScore": "8.2"
        },
        "sans20Categories": null,
        "lists": null,
        "compliances": [],
        "supportedBy": [
            "VM",
            "CA-Linux Agent"
        ],
        "vendors": [
            {
                "vendorName": "suse",
                "productName": "None"
            },
            {
                "vendorName": "opensuse",
                "productName": "None"
            }
        ],
        "vendorRefDetails": [
            {
                "vendorRef": "openSUSE-SU-2016:2994-1",
                "url": "http://lists.opensuse.org/opensuse-
updates/2016-12/msg00020.html",
                "lastModified": "1486124410000"
            }
```

```
            ],
            "vulnPatch": {
                "patchAvailable": true,
                "patchReleaseDate": "1480809600000",
                "vendorSeverity": "important",
                "patches": [
                    {
                        "id": 634478,
                        "advisoryID": "openSUSE-SU-2016:2994-1",
                        "component": null,
                        "lastModified": "1486124408000",
                        "link": "http://lists.opensuse.org/opensuse-
updates/2016-12/msg00020.html",
                        "osSoftware": "OpenSuse",
                        "rebootDetails": "Conditional",
                        "rebootRequired": 2,
                        "subComponent": null
                    }
                ]
            },
            "qidProperties": [
                "unx",
                "pci",
                "ap",
                "os"
            ]
        },
    ],
    "count": 52
}
```

Fetch Vulnerabilities Associated with a List - Bulk API

API affected	/csapi/v1.3/list/{listId}/vulns/list
Operator	GET
New or Updated APIs	New
DTD or XSD Changes	NA

Fetches vulnerabilities associated with a list. Use this API when the number of vulnerabilities is large.

Input Parameters

Parameter	Mandatory?	Data Type	Description
listId	Mandatory	string	Specify the ID or UUID of the list.
filter	Optional	string	Filter vulnerabilities by providing a query using Qualys syntax. Refer to the "How to Search" topic in the online help for assistance with creating your query.
pageSize	Optional	integer	The number of records per page to be included in the response. The default value is 50.
nextPage	Optional	integer	Specify the next page query to fetch the results of the next page. Use the value from the previous response.

Sample: Fetch Vulnerabilities Associated with a List

API Request:

```
curl -X "GET"
"<qualys_base_url>/csapi/v1.3/list/2862fff9-6b49-453f-bb66-
112a5f26c3c2/vulns/list?pageSize=50"
-H "accept: application/json"
-H "Authorization: Bearer <token>"
```

Response:

```
{
    "data": [
        {
            "description": {
```

```
                "EN": "Tenable virtual appliances deliver power, deployment
speed and all around ease of use by virtually eliminating installation,
configuration and maintenance problems.<P>\nThe Tenable Appliance contain
several vulnerabilities. One exists in the underlying operating system
kernel, two in the Appliance web interface, and multiple issues in bundled
applications.<P>\nAffected Versions:<BR>\nTenable Appliance versions
3.4.0, 3.5.0, 3.5.1, 3.10.0, 3.10.1, 4.0.0, 4.1.0, 4.2.0, 4.3.0, 4.3.1,
4.4.0 are affected.\n<P>\n\nQID Detection Logic
(Unauthenticated):<BR>\nThis QID sends a crafted HTTP request on TCP port
8000 and checks for the system response."
            },
            "consequence": {
                "EN": "Successful exploitation of these vulnerabilities
could allow an attacker to take control of the affected system."
            },
            "solution": {
                "EN": "Customers are advised to refer to <A
HREF=\"http://www.tenable.com/security/tns-2017-07\"
TARGET=\"_blank\">tns-2017-07</A> for updates pertaining to this
vulnerability."
            },
            "discoveryTypes": [
                "REMOTE"
            ],
            "published": 1495534216000,
            "updated": 1689717601000,
            "types": [
                "VULNERABILITY"
            ],
            "severity": 4,
            "risk": 40,
            "flags": [
                "REMOTE",
                "PCI_RELATED"
            ],
            "category": "CGI",
            "typeDetected": "CONFIRMED",
            "authTypes": [],
            "patches": [
                642244
            ],
            "vulnPatch": {
                "patchAvailable": true,
                "patchReleaseDate": 1488844800000,
                "vendorSeverity": "High",
                "patches": [
                    {
                        "id": 642244,
                        "advisoryID": "Tenable Appliance 4.5.0 or later
```

```
version",
                        "lastModified": 1493766004000,
                       "link": "https://www.tenable.com/products/tenable-
virtual-appliances#tos",
                        "rebootDetails": "Conditional",
                        "rebootRequired": 2
                    }
                ]
            },
            "qid": 11802,
            "exploits": [
                {
                  "name": "Linux Kernel 4.4.0 (Ubuntu) - DCCP Double-Free
(PoC) - The Exploit-DB Ref : 41457",
                    "insertDate": 1488202773000,
                    "firstSeen": 1488067200000,
                    "link": "http://www.exploit-db.com/exploits/41457",
                    "reference": "CVE-2017-6074",
                    "vendor": {
                        "name": "The Exploit-DB",
                        "link": "http://www.exploit-db.com"
                    }
                },
                ...
            ],
           "title": "Tenable Appliance Multiple Security Vulnerabilities",
            "patchAvailable": true,
            "cveIds": [
                "CVE-2017-6074",
                "CVE-2017-6543",
                "CVE-2017-8050",
                "CVE-2017-8051"
            ],
            "vendorRefs": [
                "tns-2017-07"
            ],
            "vendorRefDetails": [
                {
                    "vendorRef": "tns-2017-07",
                    "url": "http://www.tenable.com/security/tns-2017-07",
                    "urlID": 33459,
                    "lastModified": 1493766006000
                }
            ],
            "bugTraqIds": [
                "96310",
                "96418"
            ],
            "cvssInfo": {
```

```
                "baseScore": "10",
                "temporalScore": "8.3",
                "accessVector": "Network"
            },
            "cvss3Info": {
                "baseScore": "9.8",
                "temporalScore": "9.1"
            },
            "compliances": [],
            "supportedBy": [
                "VM"
            ],
            "vendors": [
                {
                    "vendorName": "linux",
                    "productName": "linux_kernel"
                },
               ...
            ],
            "qidProperties": [
                "ap",
                "noa",
                "pci",
                "lpt",
                "os"
            ]
        },
       ...
    ],
    "count": 50,
    "nextPage": [
        "988179"
    ]
}
```

Update Vulnerabilities Associated with a List

API affected	/csapi/v1.3/list/{listId}/vulns
Operator	PUT
New or Updated APIs	New
DTD or XSD Changes	NA

Updates the list of vulnerabilities/QIDs associated with a list.

Input Parameters

Parameter	Mandatory?	Data Type	Description
listId	Mandatory	string	Specify the ID or UUID of the list.
qidsAdditionFilter	Mandatory	string	Specify a filter to add QIDs to the list.
qidsAdditionFilter	Mandatory	string	Specify a filter to removed QIDs from the list.
qidsToBeAdded	Mandatory	string	Specify the QIDs to be added to the list.
qidsToBeRemoved	Mandatory	string	Specify the QIDs to be removed from the list.

Note: If QIDs are specified in "qidsToBeAdded" and "qidsToBeRemoved", the "qidsAdditionFilter" and "qidsAdditionFilter" parameters are ignored.

Sample: Update QIDs Associated with a List

API Request:

```
curl -X 'PUT'
'<qualys_base_url</csapi/v1.3/list/64b2b343-6d3c-43ba-8912-
97e45de0b460/vulns'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
-H 'Content-Type: application/json'
-d '{
  "qidsAdditionFilter": null,
  "qidsRemovalFilter": null,
  "qidsToBeAdded": [
    null
  ],
  "qidsToBeRemoved": [
    44069,
```

```
        92028
      ]
    }'
```

Response:

```
Response code 200
```

Create a Vulnerability Exception

API affected	/csapi/v1.3/exception
Operator	POST
New or Updated APIs	New
DTD or XSD Changes	NA

Creates a new vulnerability exception.

Input Parameters

Parameter	Mandatory?	Data Type	Description
name	Mandatory	string	Specify a name for the exception.
reason	Mandatory	string	Specify the reason to create the exception.
explanation	Mandatory	string	Enter explanation to support the reason for creating the exception.
scope	Mandatory	string	Specify the scope: IMAGE or CONTAINER. When the scope is IMAGE, the exception is automatically cascaded to containers spawned from the image.
listId	Mandatory	string	Specify the ID of the list to be used.
exceptionType	Mandatory	string	Specify the exception type. Currently, only VULNERABILITY is supported.
entityAssignment Request	Mandatory	string	Specify the UUID of the images to assigned to the exception. You can either specify the UUIDs directly using "idsToAdd" or specify a filter using "additionFilter". If "idsToAdd" is specified, "additionFilter" is ignored.
startDate	Mandatory	string	Specify the start date to enforce the exception.
endDate	Mandatory	string	Specify the end date for the exception.

Sample: Create a New Exception

API Request:

```
curl -X 'POST'
'<qualys_base_url>/csapi/v1.3/exception'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
-H 'Content-Type: application/json'
-d '{ "name": "VulException1", "reason": "RISK_ACCEPTED", "explanation":
"Testing API", "scope": "IMAGE", "listId": "5e586467-af10-47b8-ab26-
509ac3b823b2", "exceptionType": "VULNERABILITY",
"entityAssignmentRequest": { "idsToAdd": [ "9baf9f85-f3bf-3259-b8d5-
3cd51967d34a", "b5373ff0-044d-3004-8368-88541ae64a75" ],
"additionFilter": null }, "startDate": "1687777225000", "endDate":
"4102358400000" }'
```

Response:

```
{
  "exceptionId": "3f86db22-2a2e-4976-a947-07d575fb50d5"
}
```

Update a Vulnerability Exception

API affected	/csapi/v1.3/exception
Operator	PUT
New or Updated APIs	New
DTD or XSD Changes	NA

Updates a vulnerability exception.

Input Parameters

Parameter	Mandatory?	Data Type	Description
name	Mandatory	string	Specify a name for the exception.
reason	Mandatory	string	Specify the reason to create the exception.
explanation	Mandatory	string	Enter explanation to support the reason for creating the exception.
scope	Mandatory	string	Specify the scope: IMAGE or CONTAINER. When the scope is IMAGE, the exception is automatically cascaded to containers spawned from the image.
listId	Mandatory	string	Specify the ID of the list to be used.
exceptionType	Mandatory	string	Specify the exception type. Currently, only VULNERABILITY is supported.
entityAssignment Request	Mandatory	string	Specify the UUID of the images to assigned to the exception. You can either specify the UUIDs directly using "idsToAdd" or specify a filter using "additionFilter". If "idsToAdd" is specified, "additionFilter" is ignored.
startDate	Mandatory	string	Specify the start date to enforce the exception.
endDate	Mandatory	string	Specify the end date for the exception.

Sample: Update an Exception

API Request:

```
curl -X 'PUT'
'<qualys_base_url>/csapi/v1.3/exception/3f86db22-2a2e-4976-a947-
07d575fb50d5'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
-H 'Content-Type: application/json'
-d '{ "name": "VulException1-updated", "reason": "RISK_ACCEPTED",
"explanation": "Testing API", "scope": "IMAGE", "listId": "5e586467-af10-
47b8-ab26-509ac3b823b2", "exceptionType": "VULNERABILITY",
"entityAssignmentRequest": { "idsToAdd": [ "9baf9f85-f3bf-3259-b8d5-
3cd51967d34a", "b5373ff0-044d-3004-8368-88541ae64a75", "1f06ff34-a1e2-
381e-a29c-46e54e57c70d" ], "additionFilter": null }, "startDate":
"1687777225000", "endDate": "4102358400000" } '
```

Response:

```
{
  "exceptionId": "3f86db22-2a2e-4976-a947-07d575fb50d5"
}
```

Fetch a List of Vulnerability Exceptions

API affected	/csapi/v1.3/exception
Operator	GET
New or Updated APIs	New
DTD or XSD Changes	NA

Fetches a list of vulnerability exceptions from your account.

Sample: Fetch a List of Exceptions from Your Account

API Request:

```
curl -X 'GET'
'<qualys_base_url>/csapi/v1.3/exception?pageNumber=1&pageSize=50'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
```

Response:


```
{
  "data": [
    {
      "uuid": "760b9868-8f41-4754-b51c-0d59d27e9945",
      "name": "Test02",
      "createdBy": "rq30",
      "created": "1687519907347",
      "updatedBy": "rq30",
      "updated": "1687519907347",
      "reason": "RISK_ACCEPTED",
      "explanation": "non-impacting vulnerability",
      "scope": "IMAGE",
      "listId": "e236f17d-0ed2-4f5b-8bab-c4ae76b57f7b",
      "startDate": "1687533496914",
      "endDate": "4102358400000"
    },
    {
      "uuid": "1b4bfdd9-2ef1-4876-b5d1-7840092bb66f",
      "name": "Test01_Qflow",
      "createdBy": "rq30",
      "created": "1687514036116",
      "updatedBy": "rq30",
      "updated": "1687760549738",
      "reason": "RISK_ACCEPTED",
      "explanation": "non-impacting vulnerability",
      "scope": "IMAGE",
```

```
      "listId": "7788d038-521f-4cc8-9927-eb9b2a87ece4",
      "startDate": "1687533496914",
      "endDate": "1689379200000"
    }
  ],
  "count": 2
}
```

Fetch Details of an Exception

API affected	/csapi/v1.3/exception/{exceptionId}
Operator	GET
New or Updated APIs	New
DTD or XSD Changes	NA

Fetches details of an exception, such as scope, reason, explanation, QIDs, and list ID.

Input Parameters

Parameter	Mandatory?	Data Type	Description
exceptionId	Mandatory	string	Specify the ID or UUID of the exception.
includeQids	Optional	Boolean	Specify true if you want include QIDs associated with the exception in the exception details. By default, the value is false.

Sample: Fetch Details of an Exception

API Request:

```
curl -X 'GET'
'<qualys_base_url>/csapi/v1.3/exception/760b9868-8f41-4754-b51c-
0d59d27e9945?includeQids=false'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
```

Response:


```
{
  "exceptionId": "760b9868-8f41-4754-b51c-0d59d27e9945",
  "name": "Test02",
  "createdBy": "rq30",
  "updatedBy": "rq30",
  "created": "1687519907347",
  "updated": "1687765454244",
  "explanation": "ola",
  "reason": "RISK_ACCEPTED",
  "scope": "IMAGE",
  "imageSelectionType": "STATIC",
  "listId": "e236f17d-0ed2-4f5b-8bab-c4ae76b57f7b",
  "startDate": "1687533496914",
```

```
  "endDate": "4102358400000",
  "qids": null
}
```

Delete a Vulnerability Exception

API affected	/csapi/v1.3/exception/{exceptionId}
Operator	DELETE
New or Updated APIs	New
DTD or XSD Changes	NA

Deletes an exception.

Input Parameter

Parameter	Mandatory?	Data Type	Description
exceptionId	Mandatory	string	Specify the ID or UUID of the exception.

Sample: Delete an Exception

API Request:

```
curl -X 'DELETE'
'<qualys_base_url>/csapi/v1.3/exception/760b9868-8f41-4754-b51c-
0d59d27e9934'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
```

Response:

```
Response code 200
```

Fetch Exceptions Associated with an Image

API affected	/csapi/v1.3/images/{imageSha}/exceptions
Operator	GET
New or Updated APIs	New
DTD or XSD Changes	NA

Fetches vulnerability exceptions associated with an image.

Input Parameters

Parameter	Mandatory?	Data Type	Description
imageSha	Mandatory	string	Specify the SHA value of the image.

Sample: Fetch Exceptions Associated with an Image

API Request:

```
curl -X 'GET'
'<qualys_base_url>/csapi/v1.3/images/9bfbb2de033f1646f63fcdad40a89b13915f
0673aa19ae5494b34a826bc9935b/exceptions'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
```

Response:


```
{
  "data": [
    {
      "uuid": "77116d5b-aaa0-4dba-a334-9fe6a6f0dd98",
      "name": "Future_Exception",
      "createdBy": "rq30",
      "created": "1688364403483",
      "updatedBy": "rq30",
      "updated": "1688364723810",
      "reason": "RISK_ACCEPTED",
      "explanation": "Okay",
      "scope": null,
      "listId": "5a131be0-4a50-4233-b96d-1209f4c44ed1",
      "startDate": "1688389200000",
      "endDate": "4102358400000"
    }
  ],
  "count": 1,
  "groups": null
}
```

Update Exceptions Associated with an Image

API affected	/csapi/v1.3//images/{imageId}/exceptions
Operator	PUT
New or Updated APIs	New
DTD or XSD Changes	NA

Updates the list of exceptions mapped to an image.

Input Parameter

Parameter	Mandatory?	Data Type	Description
imageId	Mandatory	string	Specify the UUID of the image.
exceptionEvent	Mandatory	string	Specify whether to add or remove exceptions. The valid values are: ASSIGN and DEASSIGN.
exceptionIds	Mandatory	string	Specify the UUIDs of exceptions to be added or removed.

Sample

API Request:

```
curl -X 'PUT'
'<qualys_base_url>/csapi/v1.3/images/9baf9f85-f3bf-3259-b8d5-
3cd51967d34a/exceptions'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>’
-H 'Content-Type: application/json'
-d '{
  "exceptionEvent": "ASSIGN",
  "exceptionIds": [
    "c0b4ec8d-a186-4f2c-9a6d-3adc3dfb3cff"
  ]
}'
```

Response:

```
{
  "imageUuid": "9baf9f85-f3bf-3259-b8d5-3cd51967d34a"
}
```

Fetch Exceptions Associated with a Container

API affected	/csapi/v1.3/containers/{containerSha}/exceptions
Operator	GET
New or Updated APIs	New
DTD or XSD Changes	NA

Fetches vulnerability exceptions associated with a container.

Input Parameters

Parameter	Mandatory?	Data Type	Description
containerSha	Mandatory	string	Specify the SHA value of the container.

Sample: Fetch Exceptions Associated with a Container

API Request:

```
curl -X 'GET' \
'<qualys_base_url>/csapi/v1.3/containers/d1094f463df2ce4341a36c65fc4e163e
e4a6d8e474d9dd844fa20571dd421df0/exceptions' \
-H 'accept: application/json' \
-H 'Authorization: Bearer <token>'
```

Response:


```
{
  "data": [
    {
      "uuid": "c0b4ec8d-a186-4f2c-9a6d-3adc3dfb3cff",
      "name": "Test 1",
      "createdBy": "zp53",
      "created": "1687845954606",
      "updatedBy": "zp53",
      "updated": "1687845954606",
      "reason": "FALSE_POSITIVE",
      "explanation": "False positive",
      "scope": null,
      "listId": "1ef54477-eb0a-455f-b57f-ccfa18f0825d",
      "startDate": "1687860273830",
      "endDate": "4102358400000"
    },
    {
      "uuid": "d7b11c61-dcf2-4cf5-b369-8877f1b619c6",
```

```
      "name": "Test 2",
      "createdBy": "zp53",
      "created": "1687925660932",
      "updatedBy": "zp53",
      "updated": "1687936084082",
      "reason": "RISK_ACCEPTED",
      "explanation": "Risk accepted",
      "scope": null,
      "listId": "b1cfa02b-1417-4abb-bc40-bf764e009fae",
      "startDate": "1687945063571",
      "endDate": "4102358400000"
    }
  ],
  "count": 2
}
```

Update Exceptions Associated with a Container

API affected	/csapi/v1.3//containers/{containerId}/exceptions
Operator	PUT
New or Updated APIs	New
DTD or XSD Changes	NA

Updates the list of exceptions mapped to a container.

Input Parameter

Parameter	Mandatory?	Data Type	Description
containerId	Mandatory	string	Specify the UUID of the container.
exceptionEvent	Mandatory	string	Specify whether to add or remove exceptions. The valid values are: ASSIGN and DEASSIGN.
exceptionIds	Mandatory	string	Specify the UUIDs of exceptions to be added or removed.

Sample

API Request:

```
curl -X 'PUT'
'<qualys_base_url>/csapi/v1.3/containers/5081c32c-2176-3445-82ec-
7a68b9df22b6/exceptions'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
-H 'Content-Type: application/json'
-d '{ "exceptionEvent": "ASSIGN", "exceptionIds": [ "370eb9dc-bf72-4394-
bb39-6b25e1c87f3a" ] }'
```

Response:

```
{
     "ContainerUuid": "5081c32c-2176-3445-82ec-7a68b9df22b6"
}
```

List Images

API affected	/csapi/v1.3/images
Operator	GET
New or Updated APIs	Updated
DTD or XSD Changes	NA

You can view the details of exceptions associated with an image in the response.

Sample

API Request:

```
curl -X 'GET'
'<qualys_base_url>/csapi/v1.3/images?pageNumber=1&pageSize=50&sort=create
d%3Adesc'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
```

Response:

```
{
  "data": [
    {
      "created": "1687770587000",
      "updated": "1687773389415",
      "sha":
"125e16cb88d4868a1619c188d4b431e64c52be879b85d9195a1ea3da085aa70d",
      "repo": [
        {
          "registry": "docker.io",
          "tag": "rontest04",
          "repository": "qflowtest"
        }
      ],
      "repoDigests": null,
      "uuid": "2f669d85-8d36-3e9f-81ae-1c5046dadf33",
      "size": 843207849,
      "vulnerabilities": {
        "severity5Count": 12,
        "severity3Count": 169,
        "severity4Count": 25,
        "severity1Count": 2,
        "severity2Count": 5
      },
      "imageId": "125e16cb88d4",
```

```
      "associatedContainersCount": 0,
      "associatedHostsCount": 1,
      "lastVmScanDate": "1687772014637",
      "registryUuid": null,
      "source": [
        "GENERAL"
      ],
      "isDockerHubOfficial": false,
      "isInstrumented": false,
      "instrumentedFrom": null,
      "instrumentationState": null,
      "scanType": null,
      "scanTypes": [
        "DYNAMIC"
      ],
      "scanErrorCode": null,
      "scanStatus": "SUCCESS",
      "lastFoundOnHost": {
        "sensorUuid": "735c9fc4-e969-412c-b13b-c348db436275",
        "hostname": "dockercent",
        "ipAddress": "10.115.98.192",
        "uuid": "d6c12bf9-7121-46e3-92bc-f0d4183d77a8",
        "lastUpdated": "2023-06-26T09:10:05.556Z"
      },
      "exceptions": [
        "1b4bfdd9-2ef1-4876-b5d1-7840092bb66f"
      ],
      "compliance": {
        "failCount": 2,
        "passCount": 0,
        "errorCount": 0
      },
      "lastComplianceScanDate": "1687771599803"
    },
    ...
  ],
  "count": 25
}
```

Fetch Image Details

API affected	/csapi/v1.3/images/{imageSha}
Operator	GET
New or Updated APIs	Updated
DTD or XSD Changes	NA

You can view the details of exceptions associated with an image in the response.

Sample

API Request:

```
curl -X 'GET'
'<qualys_base_url>/csapi/v1.3/images/4a27414336b52cc3f423f69c453f08d86bcb
c377761d843875ba5f90bd80ed87'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
```

Response:

```
{
  "created": "1688361274000",
  "updated": "1688413525825",
  "author": "",
  "repo": [
    {
      "registry": "docker.io",
      "tag": "newtest04",
      "repository": "exception01"
    }
  ],
...
  ],
  "uuid": "e1833b20-6956-306f-8aed-7725e5edd12a",
  "sha":
"4a27414336b52cc3f423f69c453f08d86bcbc377761d843875ba5f90bd80ed87",
  "operatingSystem": "CentOS 5.11",
  "customerUuid": "7a5a4e04-1798-4a6c-80a9-64e988e382ed",
  "dockerVersion": "19.03.0-rc3",
  "size": 287952006,
  "layers": [
    {
      "size": "3276800",
      "createdBy": "/bin/bash",
      "created": "1688361274000",
```

```
      "comment": "",
      "id": "4a27414336b5",
      "sha":
"4a27414336b52cc3f423f69c453f08d86bcbc377761d843875ba5f90bd80ed87",
      "tags": [
        "exception01:newtest04"
      ]
    },
...
  "scanErrorCode": null,
  "scanStatus": "SUCCESS",
  "lastFoundOnHost": {
    "sensorUuid": "735c9fc4-e969-412c-b13b-c348db436275",
    "hostname": "dockercent",
    "ipAddress": "10.115.98.192",
    "uuid": "d6c12bf9-7121-46e3-92bc-f0d4183d77a8",
    "lastUpdated": "2023-07-03T05:14:49.859Z"
  },
  "exceptions": [
    "77116d5b-aaa0-4dba-a334-9fe6a6f0dd98"
  ],
  "softwares": [
    {
      "name": "sed",
      "version": "4.1.5-8.el5",
      "scanType": "DYNAMIC",
      "packagePath": null,
      "fixVersion": null,
      "vulnerabilities": null
    },
    ...
  ],
  "vulnerabilities": [],
  "lastComplianceScanned": "1688362358123"
}
```

List Containers

API affected	/csapi/v1.3/containers
Operator	GET
New or Updated APIs	Updated
DTD or XSD Changes	NA

You can view the details of exceptions associated with containers in the response.

Sample

API Request:

```
curl -X 'GET'
'<qualys_base_url>/csapi/v1.3/containers?pageNumber=1&pageSize=50&sort=cr
eated%3Adesc'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
```

Response:


```
{
    "data": [
      {
        "imageId": "b7e6c3064562",
        "created": "1687845624000",
        "updated": "1688030638072",
        "sha":
"d1094f463df2ce4341a36c65fc4e163ee4a6d8e474d9dd844fa20571dd421df0",
        "uuid": "05cb0e46-02d8-3e0d-b1f1-e4ad1d61da21",
        "name": "wonderful_hamilton",
        "host": {
          "sensorUuid": "aff29f6e-5c2d-425e-bff6-88427c6e991b",
          "hostname": "lxagubu",
          "ipAddress": "10.115.140.159",
          "uuid": "63000be0-00c0-0002-2851-0050568cd03b",
          "lastUpdated": "2023-06-27T06:00:48.727Z"
        },
        "state": "RUNNING",
        "imageUuid": "30bcf593-ffae-3620-bcf6-ddab50529482",
        "containerId": "d1094f463df2",
        "stateChanged": "1688030637926",
        "lastVmScanDate": "1687978936906",
        "isRoot": true,
        "vulnerabilities": {
          "severity5Count": 10,
```

```
        "severity3Count": 128,
        "severity4Count": 24,
        "severity1Count": 1,
        "severity2Count": 5
      },
      "isInstrumented": null,
      "exceptions": [
        {
          "uuid": "624efd86-6172-4851-beb1-75cb9b1634fb",
          "assignmentType": "CASCADE"
        },
        {
          "uuid": "c0b4ec8d-a186-4f2c-9a6d-3adc3dfb3cff",
          "assignmentType": "CASCADE"
        },
        {
          "uuid": "d7b11c61-dcf2-4cf5-b369-8877f1b619c6",
          "assignmentType": "MANUAL"
        }
      ],
      "compliance": {
        "failCount": 0,
        "passCount": 0,
        "errorCount": 0
      },
      "lastComplianceScanDate": null
    }
    ...
  ],
  "count": 484
}
```

Fetch Container Details

API affected	/csapi/v1.3/containers/{containerSha}
Operator	GET
New or Updated APIs	Updated
DTD or XSD Changes	NA

You can view the details of exceptions associated with a container in the response.

Sample

API Request:

```
curl -X 'GET' \
'<qualys_base_url>/csapi/v1.3/containers/d1094f463df2ce4341a36c65fc4e163e
e4a6d8e474d9dd844fa20571dd421df0' \
-H 'accept: application/json' \
-H 'Authorization: Bearer <token>'
```

Response:


```
{
    "portMapping": null,
    "imageId": "b7e6c3064562",
    "created": "1687845624000",
    "updated": "1688030638072",
    "label": [
        {
            "key": "Application",
            "value": "CheckoutApp"
        }
    ],
    "uuid": "05cb0e46-02d8-3e0d-b1f1-e4ad1d61da21",
    "sha":
"d1094f463df2ce4341a36c65fc4e163ee4a6d8e474d9dd844fa20571dd421df0",
    "privileged": false,
    "path": "/bin/bash",
    "imageSha":
"b7e6c30645628165ccd3cde23d0d4a904d464dbeabcbaf419d234755da61b7f1",
    "macAddress": "02:42:ac:11:00:02",
    "customerUuid": "1ab79f42-6cc3-757c-83d9-b0562c8a6dc8",
    "ipv4": "172.17.0.2",
    "ipv6": null,
    "name": "wonderful_hamilton",
    "host": {
        "sensorUuid": "aff29f6e-5c2d-425e-bff6-88427c6e991b",
```

```
        "hostname": "lxagubu",
        "ipAddress": "10.115.140.159",
        "uuid": "63000be0-00c0-0002-2851-0050568cd03b",
        "lastUpdated": "2023-06-27T06:00:48.727Z"
    },
    ...
    "drift": {
        "category": [],
        "reason": [],
        "software": [],
        "vulnerability": []
    },
    "vulnerabilities": [
    ...
    ],
    "isDrift": false,
    "isRoot": true,
    "lastComplianceScanned": null,
    "cluster": null,
    "cloudProvider": null,
    "exceptions": [
        {
            "uuid": "624efd86-6172-4851-beb1-75cb9b1634fb",
            "assignmentType": "CASCADE"
        },
        {
            "uuid": "c0b4ec8d-a186-4f2c-9a6d-3adc3dfb3cff",
            "assignmentType": "CASCADE"
        },
        {
            "uuid": "d7b11c61-dcf2-4cf5-b369-8877f1b619c6",
            "assignmentType": "MANUAL"
        }
    ]
}
```