Qualys Global AssetView/CyberSecurity Asset Management v2.x

API Release Notes

Version 2.14

December 20, 2022

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

URL to the Qualys API Server

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

This documentation uses the API gateway URL for Qualys US Platform 1 (https://gateway.qg1.apps.qualys.com) in sample API requests. If you're on another platform, please replace this URL with the appropriate gateway URL for your account.

New Field Added to Response of the Existing APIs

With this release, a new field “release” is added to the response of the following public V1 and V2 APIs. The “release” field is part of the OperatingSystem attributes that represents the whole version major release, minor release, and revision number for the specific kernel release of the operating system.

Public V1 APIs:

- List - am/v1/assets/host/list
- Filter List - am/v1/assets/host/filter/list
- Asset by AssetID - am/v1/asset/host/id

Public V2 APIs:

- Filter List - /rest/2.0/search/am/asset
- Asset by AssetID - /rest/2.0/get/am/asset

Response:

```
{
  "responseMessage": "Valid API Access",
  "count": 1,
  "responseCode": "SUCCESS",
  "lastSeenAssetId": 18302027,
  "hasMore": 0,
  "assetListData": {
    "asset": [
      {
        "assetId": 18302027,
        "assetUUID": "6324f729-0321-0002-940f-0050568cd03b",
        "hostId": 2992008,
        "lastModifiedDate": "2022-11-18T05:21:22.000Z",
        "agentId": "6324f729-0321-0002-940f-0050568cd03b",
        "createdDate": "2022-11-10T17:58:28.000Z",
        "sensorLastUpdatedDate": "2022-11-18T05:21:22.000Z",
       ...
        "operatingSystem": {
          "osName": "CentOS Linux 7.4.1708",
          "fullName": "The CentOS Project CentOS 7 (1708)",
          "category": "Linux / Server",
          "category1": "Linux",
          "category2": "Server",
          "productName": "CentOS",
          "publisher": "The CentOS Project",
          "edition": null,
          "marketVersion": "7",
          "version": "1708",
          "update": null,
          "architecture": "x86_64",
          "lifecycle": {
            "gaDate": "2017-09-13T07:00:00.000Z",
            "eolDate": "2020-08-06T07:00:00.000Z",
            "eosDate": "2024-06-30T07:00:00.000Z",
            "stage": "EOL",
            "lifeCycleConfidence": "Exact",
            "eolSupportStage": "Full updates",
            "eosSupportStage": "Maintenance Updates"
          },
          "taxonomy": {
            "id": null,
            "name": "Linux / Server",
            "category1": "Linux",
            "category2": "Server"
          },
          "productUrl":
"https://www.centos.org/,https://en.wikipedia.org/wiki/CentOS,",
          "productFamily": null,
          "installDate": "2018-08-01T05:54:44.000Z",
          "release": "7.4.1708"
        },
        ...

      }
    ]
  }
}
```

Assets Listing and Assets Count Based on User Scope

Before the CSAM 2.14.0.0 release, it was possible to define the user scoping for the public V2 APIs only.

With this release, the user scoping can now be defined for the public V1 APIs too.

For the following V1 APIs, the assets list and count are now shown based on the scope defined for the respective user. After the scope is defined for a respective user, that user can access only those assets, which are tagged by the specified tags.

- am/v1/assets/host/list
- am/v1/assets/host/count
- /am/v1/asset/host/id?assetId=<asset_id>
- /am/v1/assets/host/filter/list?filter=<Filter>

Sample - Get a list of assets

API Request:

```
curl --location --request POST
'https://gateway.qg1.apps.qualys.com/am/v1/assets/host/list' \--header
'Authorization: Bearer <Token>'
```

Response:

```
{
    "responseMessage": "Valid API Access",
    "count": 3,
    "responseCode": "SUCCESS",
    "lastSeenAssetId": 7626816,
    "hasMore": 0,
    "assetListData": {
        "asset": [
            {
                "assetId": 7624721,
                "assetUUID": "58c0b26c-5ecf-4b99-bce6-513096b80ce9",
                "hostId": 1535674,
                ...
                "operatingSystem": {
                    "osName": "Red Hat Enterprise Linux 8.4",
                    "fullName": "Red Hat Enterprise Linux 8.4",
                    ...
                    },
                    "taxonomy": {
                        "id": null,
                        "name": "Linux / Unidentified",
                        "category1": "Linux",
                        "category2": "Unidentified"
                    },
                    "productUrl":
"https://access.redhat.com/support/policy/updates/errata#Maintenance_Supp
ort_2_Phase,https://access.redhat.com/articles/3078,https://www.linkedin.
com/pulse/how-update-red-hat-enterprise-linux-via-minor-releases-
blasco/",
                    "productFamily": null,
                    "installDate": "2019-01-08T23:00:23.000Z",
                    "release": "8.4"
                },
                "hardware": {
                    "fullName": null,
                    "category": "Computers / Unidentified",
                    "category1": "Computers",
                    ...
                    },
                    "taxonomy": {
                        "id": null,
                        "name": "Computers / Unidentified",
                        "category1": "Computers",
                        "category2": "Unidentified"
                    },
                    "productUrl": ",,",
                    "productFamily": null
                },
                "userAccountListData": {
                    "userAccount": [
                        {
                            "name": "Administrator"
                        },
                        ...
                        }
                      ]
                 }
             ]
       }
}
```

Sample - Get a count of assets

API Request:

```
curl --location --request POST
'https://gateway.qg1.apps.qualys.com/am/v1/assets/host/count' \--header
'Authorization: Bearer <Token>'
```

Response:

```
{
    "count": 3,
    "responseCode": "SUCCESS",
    "responseMessage": "Valid API Access"
}
```

Note: If the API Access is not provided to a user, then the following response is shown:

```
{
    "responseMessage": "User doesn not have permission to access API
module",
    "count": 0,
    "responseCode": "SUCCESS",
    "lastSeenAssetId": null,
    "hasMore": 0,
    "assetListData": null
}
```

Dynamic Tag Rule Creation Using Global Asset View Tag Rule Engine

With this release, you can now create and update dynamic tag rule using GLOBAL_ASSET_VIEW tag rule engine. For more information, refer to the Cloud Platform 3.14 API Release Notes.

GET List of Vulnerabilities Discovered by EASM

API affected	/rest/2.0/search/am/easm/vulns
New or Updated APIs	New
Operator	Post
DTD or XSD changes	No

With this release, we have added a new API that helps you to get a list of vulnerabilities discovered by EASM.

Input Parameters

By using the following input parameters, you can now find assets with vulnerabilities with specific CVEID, CVSS, and QVS..

Parameter	Description
`asset.assetId` (Integer)	Provide the asset Id for which you want to get the list of vulnerabilities.
`asset.ipaddress` (String)	Provide the IP address of the asset for which you want to get the list of vulnerabilities.
`vulnerability.cveId` (Integer)	Provide the cveId of the vulnerability.
`vulnerability.type` (String)	Provide the vulnerability type, for example - Potential.
`vulnerability.cvss` (Integer)	Provide the cvss score of the vulnerability.
`vulnerability.qvs` (Integer)	Provide the qvs score of the vulnerability.

Sample - Get a list of assets with vulnerabilities with specific CVEID, CVSS, and QVS

API Request without filter:

```
curl --location --request POST
'https://gateway.qg1.apps.qualys.com/rest/2.0/search/am/easm/vulns' \ --header
'Authorization: Bearer <JWT Token>' \--data-raw ''
```

Response

```
{
    "responseMessage": "Valid API Access",
    "count": 2,
    "responseCode": "SUCCESS",
    "lastSeenVulnId": 16972,
    "hasMore": 0,
    "externalVulnerabilityListData": {
        "vulnerability": [
            {
                "ipaddress": "10.100.152.200",
                "assetId": 19047900,
                "vulnId": 16971,
                "cveId": "CVE-2016-20012",
                "type": "Potential",
                "summary": "** DISPUTED ** OpenSSH through 8.7 allows
remote attackers, who have a suspicion that a certain combination of
username and public key is known to an SSH server, to test whether this
suspicion is correct. This occurs because a challenge is sent only when
that combination could be valid for a login session. NOTE: the vendor does
not recognize user enumeration as a vulnerability for this product.",
                "lastUpdated": "2022-12-14",
                "qvs": 37,
                "cvss": 5.3
            },
            {
                "ipaddress": "10.100.152.200",
                "assetId": 19047900,
                "vulnId": 16972,
                "cveId": "CVE-2017-15906",
                "type": "Potential",
                "summary": "The process_open function in sftp-server.c in
OpenSSH before 7.6 does not properly prevent write operations in readonly
mode, which allows attackers to create zero-length files.",
                "lastUpdated": "2022-12-14",
                "qvs": 30,
                "cvss": 5.3
            },
}
}
```

API Request with filter in XML format:

Refer to the following example, wherein you can see a sample request to get all assets with vulnerabilities with CVSS greater then 9.

```
curl --location --request POST
'https://gateway.qg1.apps.qualys.com/rest/2.0/search/am/easm/vulns' \
--header 'Authorization: Bearer <JWT Token> ' \
--header 'Content-Type: application/xml' \
--data-raw '<FilterRequest>
    <filters>
        <Criteria field="vulnerability.cvss" operator="GREATER">
            <value>9</value>
        </Criteria>
    </filters>
</FilterRequest>'
```

Response

```
{
    "responseMessage": "Valid API Access",
    "count": 2,
    "responseCode": "SUCCESS",
    "lastSeenVulnId": 17060,
    "hasMore": 0,
    "externalVulnerabilityListData": {
        "vulnerability": [
            {
                "ipaddress": "20.100.300.600",
                "assetId": 19046733,
                "vulnId": 17046,
                "cveId": "CVE-2017-9120",
                "type": "Potential",
                "summary": "PHP 7.x through 7.1.5 allows remote attackers
to cause a denial of service (buffer overflow and application crash) or
possibly have unspecified other impact via a long string because of an
Integer overflow in mysqli_real_escape_string.",
                "lastUpdated": "2022-12-14",
                "qvs": 72,
                "cvss": 9.8
            },
            {
                "ipaddress": "20.100.300.600",
                "assetId": 19046733,
                "vulnId": 17060,
                "cveId": "CVE-2021-21708",
                "type": "Potential",
              "summary": "In PHP versions 7.4.x below 7.4.28, 8.0.x below
8.0.16, and 8.1.x below 8.1.3, when using filter functions with
FILTER_VALIDATE_FLOAT filter and min/max limits, if the filter fails,
there is a possibility to trigger use of allocated memory after free,
which can result it crashes, and potentially in overwrite of other memory
chunks and RCE. This issue affects: code that uses FILTER_VALIDATE_FLOAT
with min/max limits.",
                "lastUpdated": "2022-12-14",
                "qvs": 72,
                "cvss": 9.8
            },
        ]
    }
}
```

API Request with filter in JSON format:

Refer to the following example, wherein you can see the sample request to get all assets with vulnerabilities with CVE-ID : CVE-2016-20012.

curl --location --request POST
'https://gateway.qg1.apps.qualys.com/rest/2.0/search/am/easm/vulns' \--header
'Authorization: Bearer <JWT Token>

```
curl --location --request POST
'https://gateway.qg1.apps.qualys.com/rest/2.0/search/am/easm/vulns' \
--header 'Authorization: Bearer <JWT Token>' \
--header 'Content-Type: application/json' \
--data-raw '{
  "filters": [
       {
      "field": "vulnerability.cveId",
      "operator": "EQUALS",
      "value": "CVE-2016-20012"
    }
  ]
}'
```

Response

```
{
  "responseMessage": "Valid API Access",
  "count": 2,
  "responseCode": "SUCCESS",
  "lastSeenVulnId": 17043,
  "hasMore": 0,
  "externalVulnerabilityListData": {
    "vulnerability": [
      {
        "ipaddress": "10.100.152.200",
        "assetId": 19047900,
        "vulnId": 16971,
        "cveId": "CVE-2016-20012",
        "type": "Potential",
        "summary": "** DISPUTED ** OpenSSH through 8.7 allows remote
attackers, who have a suspicion that a certain combination of username and
public key is known to an SSH server, to test whether this suspicion is
correct. This occurs because a challenge is sent only when that
combination could be valid for a login session. NOTE: the vendor does not
recognize user enumeration as a vulnerability for this product.",
        "lastUpdated": "2022-12-14",
        "qvs": 37,
        "cvss": 5.3
      },
      {
        "ipaddress": "20.100.300.600",
        "assetId": 19046733,
        "vulnId": 17043,
        "cveId": "CVE-2016-20012",
        "type": "Potential",
        "summary": "** DISPUTED ** OpenSSH through 8.7 allows remote
attackers, who have a suspicion that a certain combination of username and
public key is known to an SSH server, to test whether this suspicion is
correct. This occurs because a challenge is sent only when that
combination could be valid for a login session. NOTE: the vendor does not
recognize user enumeration as a vulnerability for this product.",
        "lastUpdated": "2022-12-14",
        "qvs": 37,
        "cvss": 5.3
      }
    ]
  }
}
```

Request with multiple filters

Refer to the following example, wherein you can see the sample request to get all assets with vulnerabilities type as ’Potential’ and cvss greater than 8.

```
curl --location --request POST
'https://gateway.qg1.apps.qualys.com/rest/2.0/search/am/easm/vulns' \
--header 'Authorization: Bearer <JWT Token>' \
--header 'Content-Type: application/json' \
--data-raw '{
  "filters": [
        {
      "field": "vulnerability.type",
      "operator": "EQUALS",
      "value": "Potential"
    },
    {
      "field": "vulnerability.cvss",
      "operator": "GREATER",
      "value": "8"
    }
  ],
  "operation": "AND"
}'
```

Response

```
{
  "responseMessage": "Valid API Access",
  "count": 2,
  "responseCode": "SUCCESS",
  "lastSeenVulnId": 17068,
  "hasMore": 0,
  "externalVulnerabilityListData": {
    "vulnerability": [
      {
        "ipaddress": "20.100.300.600",
        "assetId": 19046733,
        "vulnId": 17046,
        "cveId": "CVE-2017-9120",
        "type": "Potential",
       "summary": "PHP 7.x through 7.1.5 allows remote attackers to cause
a denial of service (buffer overflow and application crash) or possibly
have unspecified other impact via a long string because of an Integer
overflow in mysqli_real_escape_string.",
        "lastUpdated": "2022-12-14",
        "qvs": 72,
        "cvss": 9.8
      },
      {
        "ipaddress": "20.100.300.600",
        "assetId": 19046733,
        "vulnId": 17068,
        "cveId": "CVE-2022-37454",
        "type": "Potential",
        "summary": "The Keccak XKCP SHA-3 reference implementation before
fdc6fef has an integer overflow and resultant buffer overflow that allows
attackers to execute arbitrary code or eliminate expected cryptographic
properties. This occurs in the sponge function interface.",
        "lastUpdated": "2022-12-14",
        "qvs": 72,
        "cvss": 9.8
      }
    ]
  }
```

Note:

- The following operators are supported for 'vulnerability.cvss' and 'vulnerability.qvs':

EQUALS, IN, NOT_EQUALS, GREATER, LESSER, GREATER_THAN_EQUAL, LESS_THAN_EQUAL

- Page Size for Response will be 1000. The lastSeenVulnId can be used for pagination.

Example:

```
https://gateway.qg1.apps.qualys.com/rest/2.0/search/am/easm/vulns?lastSee
nVulnId=17068
```

Here, lastSeenVulnID is the VulnID of the last CVE in response where VulnID is a unique identifier created for each CVE. It does not have any other significance.

- Provide multiple values as a comma separated list and also use the IN Operator.

Example:

```
{
  "filters": [
            {
      "field": "vulnerability.cveId",
      "operator": "IN",
      "value": "CVE-2021-21707,CVE-2021-21708"
    }
  ]
}
```

Exclusion of Domain and Subdomain from EASM Profile

API affected	/easm/v1/profile/
New or Updated APIs	Updated
Operator	Post, Put, and Patch
DTD or XSD changes	No

With this release, you can exclude certain domains and subdomains from the existing EASM profile.

Sample - Exclude required domains and subdomains from the existing EASM profile

<u>API Request with the Post operator</u>

```
curl --location --request POST
'https://gateway.qg1.apps.qualys.com/easm/v1/profile' \
--header 'Authorization: Bearer <JWT Token>' \
--header 'Content-Type: application/json' \
--data-raw '{
    "includeSeeds": [
        {
            "seedType": "ORGANIZATION",
            "seedValue": "Qualys, Inc",
            "seedHeading": null,
            "enumerateSubsidiary": true,
            "horizontalEnumeration": true,
            "seedFilters": []
        },
        {
            "seedType": "DOMAIN",
            "seedValue": "qualys.com",
            "seedHeading": null,
            "enumerateSubsidiary": true,
            "horizontalEnumeration": true,
            "seedFilters": []
        }
    ],
    "excludeSeeds": [
        {
            "seedType": "DOMAIN",
            "seedValue":
"hightechnologycouncil.com;usecases.totalcloud.io"
        },
{
            "seedType": "DOMAIN",
            "seedValue": "lps.qualys.com;totalcloud.io"
        }
    ]
}'
```

Response

```
{
    "code": "201",
    "status": "SAVED",
    "date": "2022-12-15 07:17:59",
    "message": "Profile Created Successfully: "
}
```