

# Vulnerability Note API

Please file issues using [VINCE](#) or [GitHub](#).

- [Authentication](#)
- [Code Examples](#)
  - [Get Vulnerability Note content](#)
  - [Get summary Vulnerability Notes for time period](#)

## Authentication

The Vulnerability Note API is different from the [VINCE API](#). The Vulnerability Note API does not require authentication, Vulnerability Notes are public.

## Code Examples

### Get Vulnerability Note content

```
#
# get content for VU#257161
#
https://kb.cert.org/vuls/api/257161/
{
  "vuid": "VU#257161",
  "idnumber": "257161",
  "name": "Treck IP stacks contain multiple vulnerabilities",
  "keywords": null, ...

#
# get vulnerabilities for VU#257161
#
https://kb.cert.org/vuls/api/257161/vuls/
{
  "note": "257161",
  "cve": "2020-11907",
  "description": "Improper Handling of Length Parameter Inconsistency (CWE-130) in TCP component. A remote
attacker can send a malformed TCP packet that can cause trigger an integer underflow event leading to
unexpected behavior of a crash or segmentation fault on the target device.",
  "uid": "CVE-2020-11907",
  "case_increment": 12,
  "date_added": "2020-06-16T17:13:46.826755Z",
  "dateupdated": "2021-02-25T18:15:04.627659Z"
}, ....

#
# get vendors (including status and statements) for VU#257161
#
https://kb.cert.org/vuls/api/257161/vendors/
{
  "note": "257161",
  "contact_date": "2020-05-07T17:38:23Z",
  "vendor": "SonicWall",
  "references": "",
  "statement": "",
  "dateupdated": "2021-02-25T18:15:20.742422Z",
  "statement_date": null,
  "addendum": "Sonicwall has mentioned that Treck stack is not in use in their SonicOS\r\nhttps://community.
sonicwall.com/technology-and-support/discussion/931/about-ripple20"
}, ....

#
# get vendor/vul status for VU#257161
# this will list the vendor status for each vulnerability identified
#
https://kb.cert.org/vuls/api/257161/vendors/vuls/
{
```

```

"vul": "CVE-2020-11907",
"vendor": "QNAP",
"status": "Not Affected",
"date_added": "2020-10-08T14:58:54.963610Z",
"dateupdated": "2021-02-25T18:15:11.244358Z",
"references": null,
"statement": null
}, ...

#
# search by CVE ID
#
https://kb.cert.org/vuls/api/vuls/cve/2020-11907/
{
  "vulnerability": {
    "note": "257161",
    "cve": "2020-11907",
    "description": "Improper Handling of Length Parameter Inconsistency (CWE-130) in TCP component. A remote
attacker can send a malformed TCP packet that can cause trigger an integer underflow event leading to
unexpected behavior of a crash or segmentation fault on the target device.",
    "uid": "CVE-2020-11907",
    "case_increment": 12,
    "date_added": "2020-06-16T17:13:46.826755Z",
    "dateupdated": "2021-02-25T18:15:04.627659Z"
  },
  "note": {
    "vuid": "VU#257161",
    ...
  },
  "vendors": [
    {
      "vul": "CVE-2020-11907",
      "vendor": "QNAP",
      "status": "Not Affected",
      "date_added": "2020-10-08T14:58:54.963610Z",
      "dateupdated": "2021-02-25T18:15:11.244358Z",
      "references": null,
      "statement": null
    },
    ...
  ]
}

```

Get summary Vulnerability Notes for time period

```
#
# get summary of Vulnerability Notes published in 2020
#
https://kb.cert.org/vuls/api/2010/summary/
{
  "count": 40,
  "notes": [
    "VU#498544",
    "VU#491944",
    "VU#335217",
    "VU#962085",
    ...
  ]
}

#
# get summary for December 2020
#
https://kb.cert.org/vuls/api/2020/12/summary/
{
  "count": 3,
  "notes": [
    "VU#815128",
    "VU#429301",
    "VU#843464"
  ]
}

#
# get Vulnerability Notes published in December 2020
#
https://kb.cert.org/vuls/api/2020/12/

#
# get vendors listed in Vulnerability Notes published in November 2010
#
https://kb.cert.org/vuls/api/vendors/2010/11/summary/

#
# get all vendor records published in November 2010
#
https://kb.cert.org/vuls/api/vendors/2010/11/
```