Vulnerability Note API

Please file issues using VINCE or GitHub.

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/
```

Get a specific Vulnerability Advisory in CSAF format

```
#
# get CSAF format of advisory for VU#495801
# https: //kb.cert.org/vuls/api/495801/csaf/
{
    "document": {
        "acknowledgments": [
            {
                "urls": [
                    "https://kb.cert.org/vuls/id/495801#acknowledgements"
                ]
            }
        ],
        "category": "CERT/CC Vulnerability Note",
        "csaf_version": "2.0",
        "notes": [
            {
                "category": "summary",
                "text": "### Overview\r\n\r\nVersions 1.1.5 and earlier of the mu HTTP deamon (muhttpd) are
vulnerable to path traversal via crafted HTTP request from an unauthenticated user. This vulnerability can
```

```
allow unauthenticated users to download arbitrary files and collect private information on the target
device.....",
                "title": "Summary"
            },
            {
                "category": "legal_disclaimer",
                "text": "THIS DOCUMENT IS PROVIDED ON AN 'AS IS' BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE
OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE
INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. ",
                "title": "Legal Disclaimer"
            },
            {
                "category": "other",
                "text": "CERT/CC Vulnerability Note is a limited advisory. It primarily identifies vendors
impacted by the advisory and not specific products. We only support \"known_affected\" and \"
known_not_affected\" status. Please consult the vendor's statements and advisory URL if provided by the vendor
for more details ",
                "title": "Limitations of Advisory"
            }
        ],
        "publisher": {
            "category": "coordinator",
            "contact_details": "Email: cert@cert.org, Phone: +1412 268 5800",
            "issuing_authority": "CERT/CC under DHS/CISA https://www.cisa.gov/cybersecurity also see https://kb.
cert.org/ ",
            "name": "CERT/CC",
            "namespace": "https://kb.cert.org/"
        },
        "references": [
            {
                "url": "https://vuls.cert.org/confluence/display/Wiki/Vulnerability+Disclosure+Policy",
                "summary": "CERT/CC vulnerability disclosure policy"
            },
            {
                "summary": "CERT/CC document released",
                "category": "self",
                "url": "https://kb.cert.org/vuls/id/495801"
            },
            {
                "url": "https://derekabdine.com/blog/2022-arris-advisory",
                "summary": "https://derekabdine.com/blog/2022-arris-advisory"
            },
            {
                "url": "https://blog.malwarebytes.com/exploits-and-vulnerabilities/2022/08/millions-of-arris-
routers-are-vulnerable-to-path-traversal-attacks",
                "summary": "https://blog.malwarebytes.com/exploits-and-vulnerabilities/2022/08/millions-of-
arris-routers-are-vulnerable-to-path-traversal-attacks"
            },
            {
                "url": "https://www.cisa.gov/uscert/ncas/tips/ST15-002",
                "summary": "https://www.cisa.gov/uscert/ncas/tips/ST15-002"
            }
        ],
        "title": "muhttpd versions 1.1.5 and earlier are vulnerable to path traversal",
        "tracking": {
            "current_release_date": "2022-08-05 20:02:52.605648+00:00",
            "generator": {
                "engine": {
                    "name": "VINCE",
                    "version": "1.50.3"
                }
            },
            "id": "VU#495801",
            "initial_release_date": "2022-08-04 18:22:24.069865+00:00",
            "revision_history": [
                {
                    "date": "2022-08-05 20:02:52.605648+00:00",
                    "number": "1.20220805200252.2",
                    "summary": "Released on 2022-08-05 20:02:52.605648+00:00"
                }
            ],
```

```
            "status": "final",
            "version": "1.20220805200252.2"
        }
    },
    "vulnerabilities": [
        {
            "title": "The base firmware for this modem contains an MIT-licensed web server from an individual
developer called \"muhttpd.",
            "notes": [
                {
                    "category": "summary",
                    "text": "The base firmware for this modem contains an MIT-licensed web server from an
individual developer called \"muhttpd.\" This server has been unmaintained since 2010. The server has a path
traversal vulnerability that allows any file on the modem to be read as root"
                }
            ],
            "cve": "CVE-2022-31793",
            "ids": [
                {
                    "system_name": "CERT/CC V Identifier ",
                    "text": "VU#495801"
                }
            ],
            "product_status": {
                "known_not_affected": [
                    "CSAFPID-eb07f774-32d4-11ed-aeca-0aa659cdc35f"
                ]
            }
        }
    ],
    "product_tree": {
        "branches": [
            {
                "category": "vendor",
                "name": "AT&T",
                "product": {
                    "name": "AT&T Products",
                    "product_id": "CSAFPID-eb07f774-32d4-11ed-aeca-0aa659cdc35f"
                }
            },
            {
                "category": "vendor",
                "name": "SaskTel",
                "product": {
                    "name": "SaskTel Products",
                    "product_id": "CSAFPID-eb082dc0-32d4-11ed-aeca-0aa659cdc35f"
                }
            }
        ]
    }
}
```