Securing the Open Source Software Supply Chain

PyCon US 2022

@di_codes

Hi, I'm Dustin

- Software Engineer, Google Open Source Security Team (GOSST)
- Director, Python Software Foundation
- Maintainer, Python Package Index

Part 1:

Q&A

Is it *safe* to use open-source software?

Is it safe to use open-source software?

Yes!

Is it safe to use open-source software?

Yes![*]

[*] Use only as directed. Open source software is not guaranteed to be safe and usually amounts to allowing strangers to run arbitrary code on your machine. Don't talk to strangers. Talk to your doctor if you are considering switching to an ecosystem with more security guarantees. Any ecosystem claiming to be more secure probably can't make those guarantees anyway. All software is vulnerable, all we can do is accept the inevitable reality of bugs, outages, vulnerabilities, and the heat death of the universe. We don't make mistakes, we just have happy little accidents. Exposure to vulnerabilities may prevent you from ever trusting any software ever again. Closed-source software isn't less vulnerable, it just gets less press. Open source doesn't have a security problem, it has a sustainability problem. Don't blame the maintainers, pay the maintainers. Apply security patches directly to the forehead. If your job doesn't let you use open source, apply directly for a new job. Exposure to open source may lower your expectations. Remember: if you expect nothing from anybody, you're never disappointed. Void where prohibited. Not all practices described in this talk are applicable to all persons or at all locations. Literally nothing you do will void the warranty, because there is no warranty. Use of open source may cause upset stomach, headache, and hot takes on Twitter.

A better question:

How can we use open-source software safely?

What is the Software Supply Chain?

The Software Supply Chain:

Everything it takes to produce your software

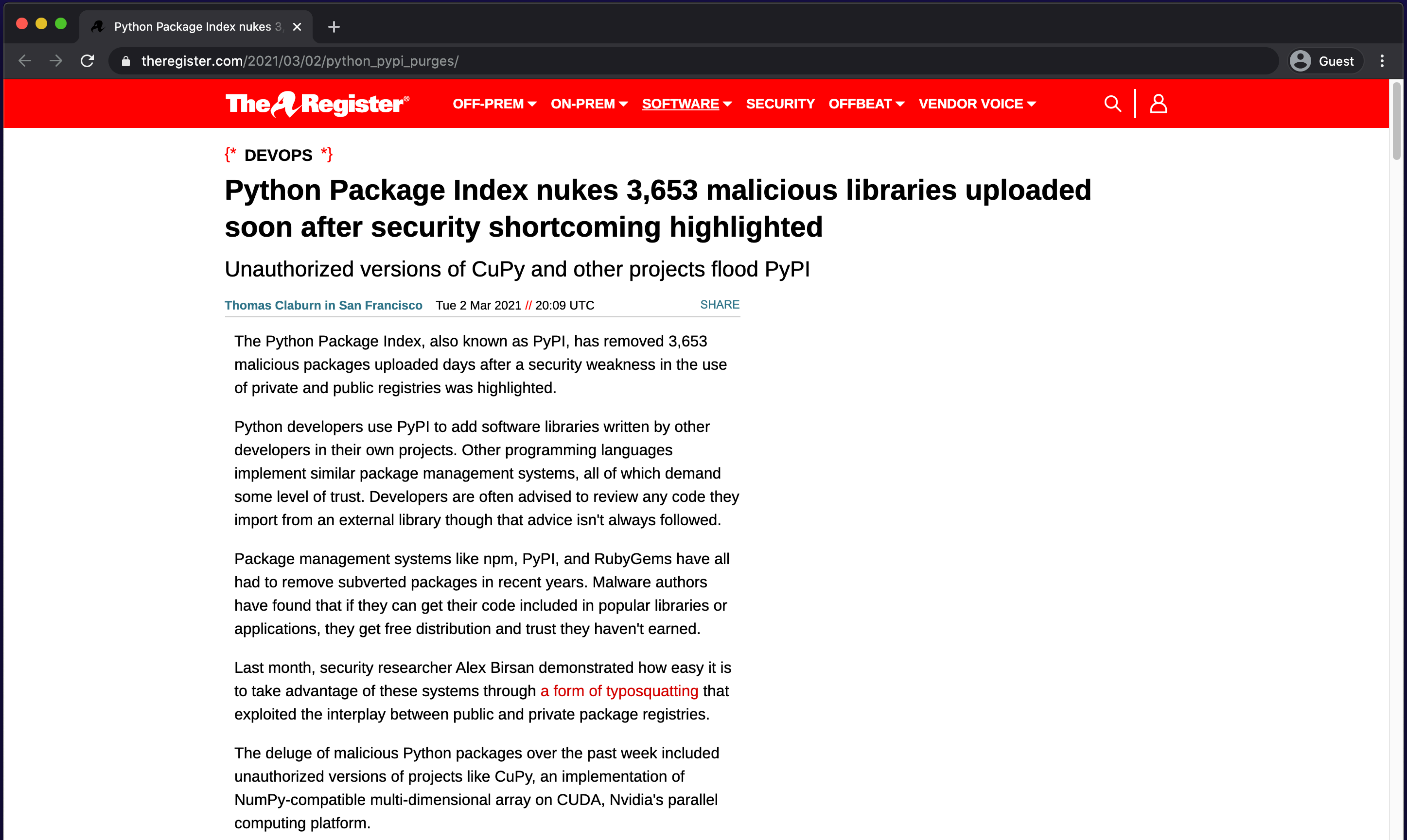
What is the *Secure* Software Supply Chain?

The Secure Software Supply Chain:

All those things, and they're definitely not compromised

Why is software-supply chain security such a big deal?

Why is software-supply chain security such a big deal *right now*?


Python Package Index nukes 3,
theregister.com/2021/03/02/python_pypi_purges/
Guest
The Register®
OFF-PREM
ON-PREM
SOFTWARE
SECURITY
OFFBEAT
VENDOR VOICE

{* DEVOPS *}

Python Package Index nukes 3,653 malicious libraries uploaded soon after security shortcoming highlighted

Unauthorized versions of CuPy and other projects flood PyPI

Thomas Claburn in San Francisco   Tue 2 Mar 2021 // 20:09 UTC   SHARE

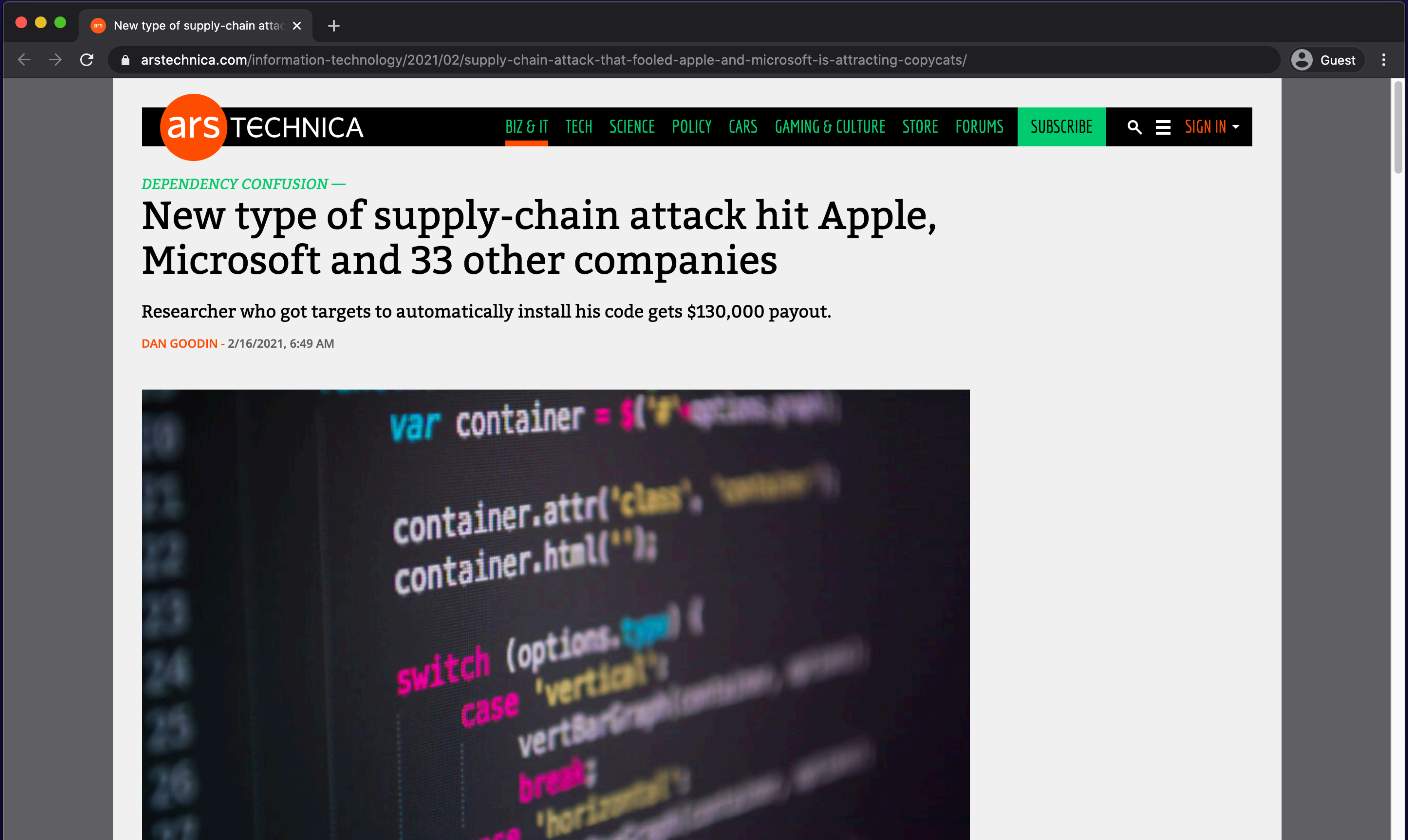
The Python Package Index, also known as PyPI, has removed 3,653 malicious packages uploaded days after a security weakness in the use of private and public registries was highlighted.

Python developers use PyPI to add software libraries written by other developers in their own projects. Other programming languages implement similar package management systems, all of which demand some level of trust. Developers are often advised to review any code they import from an external library though that advice isn't always followed.

Package management systems like npm, PyPI, and RubyGems have all had to remove subverted packages in recent years. Malware authors have found that if they can get their code included in popular libraries or applications, they get free distribution and trust they haven't earned.

Last month, security researcher Alex Birsan demonstrated how easy it is to take advantage of these systems through a form of typosquatting that exploited the interplay between public and private package registries.

The deluge of malicious Python packages over the past week included unauthorized versions of projects like CuPy, an implementation of NumPy-compatible multi-dimensional array on CUDA, Nvidia's parallel computing platform.



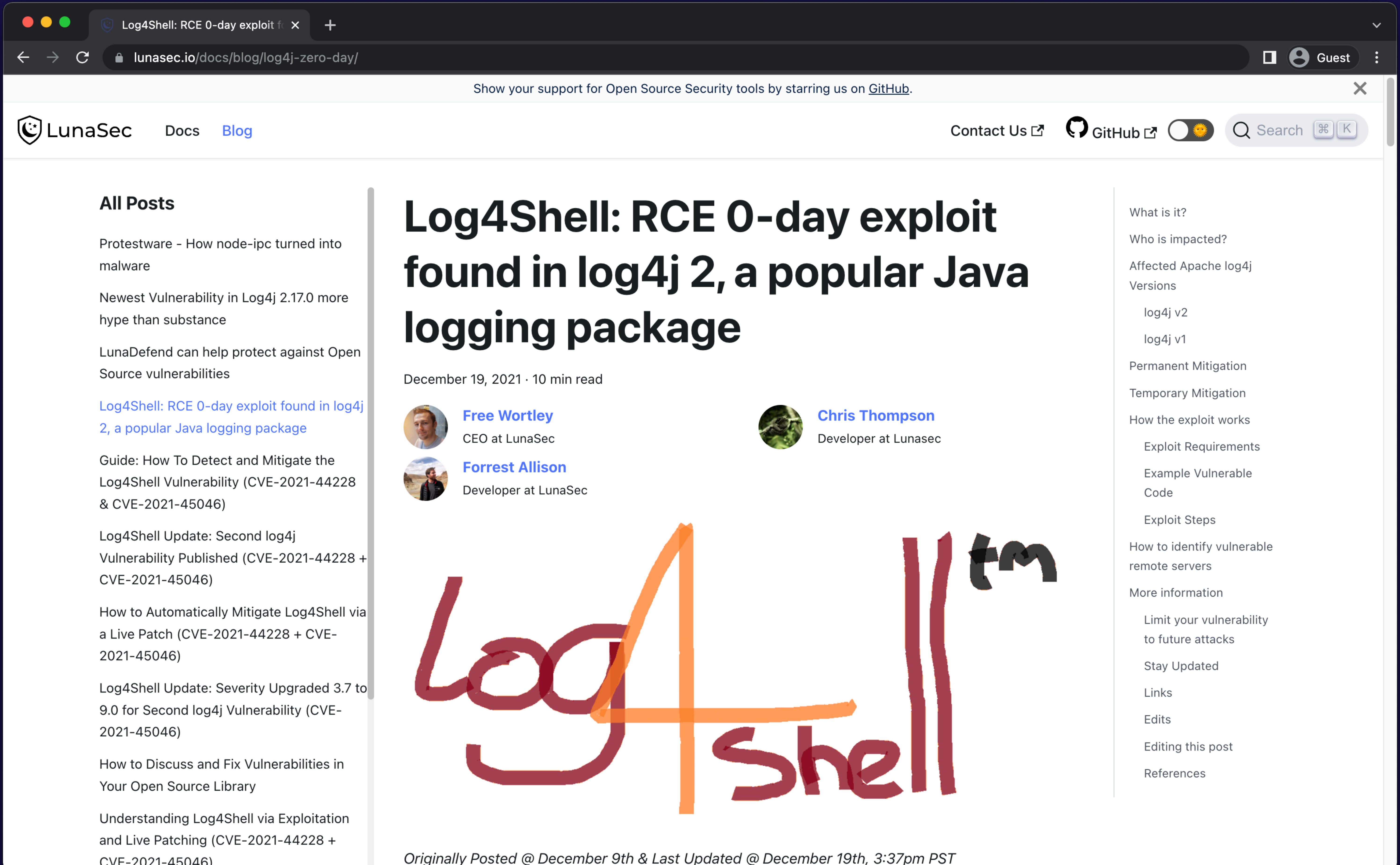
New type of supply-chain attac
arstechnica.com/information-technology/2021/02/supply-chain-attack-that-fooled-apple-and-microsoft-is-attracting-copycats/
Guest

DEPENDENCY CONFUSION —

New type of supply-chain attack hit Apple, Microsoft and 33 other companies

Researcher who got targets to automatically install his code gets $130,000 payout.

DAN GOODIN - 2/16/2021, 6:49 AM


Log4Shell: RCE 0-day exploit f
lunasec.io/docs/blog/log4j-zero-day/
Guest

All Posts

Protestware - How node-ipc turned into malware

Newest Vulnerability in Log4j 2.17.0 more hype than substance

LunaDefend can help protect against Open Source vulnerabilities

Log4Shell: RCE 0-day exploit found in log4j 2, a popular Java logging package

Guide: How To Detect and Mitigate the Log4Shell Vulnerability (CVE-2021-44228 & CVE-2021-45046)

Log4Shell Update: Second log4j Vulnerability Published (CVE-2021-44228 + CVE-2021-45046)

How to Automatically Mitigate Log4Shell via a Live Patch (CVE-2021-44228 + CVE-2021-45046)

Log4Shell Update: Severity Upgraded 3.7 to 9.0 for Second log4j Vulnerability (CVE-2021-45046)

How to Discuss and Fix Vulnerabilities in Your Open Source Library

Understanding Log4Shell via Exploitation and Live Patching (CVE-2021-44228 + CVE-2021-45046)

Log4Shell: RCE 0-day exploit found in log4j 2, a popular Java logging package

December 19, 2021 · 10 min read

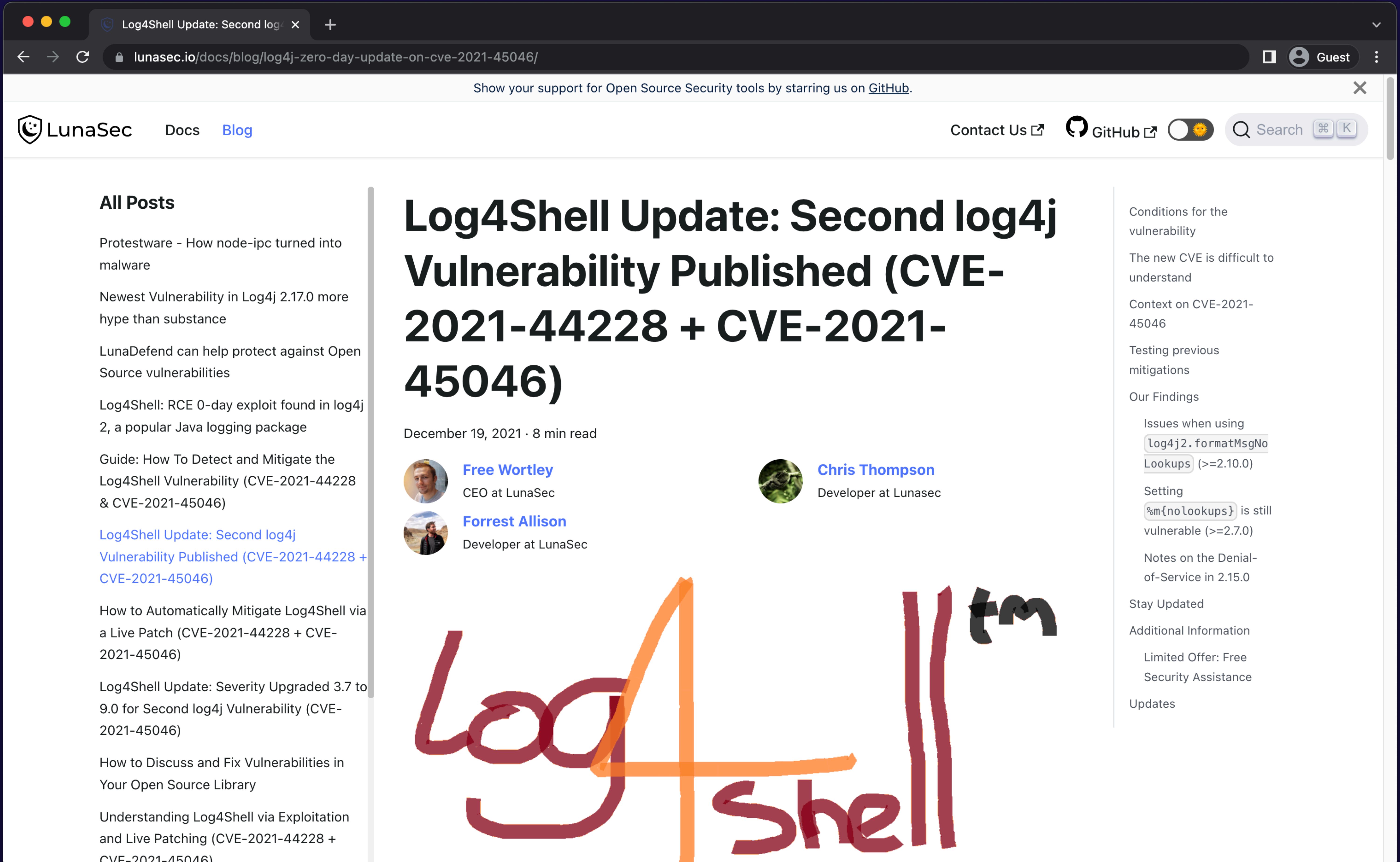
Free Wortley
CEO at LunaSec

Chris Thompson
Developer at Lunasec

Forrest Allison
Developer at LunaSec

Originally Posted @ December 9th & Last Updated @ December 19th, 3:37pm PST

What is it?
Who is impacted?
Affected Apache log4j Versions
log4j v2
log4j v1
Permanent Mitigation
Temporary Mitigation
How the exploit works
Exploit Requirements
Example Vulnerable Code
Exploit Steps
How to identify vulnerable remote servers
More information
Limit your vulnerability to future attacks
Stay Updated
Links
Edits
Editing this post
References


Log4Shell Update: Second log4j
lunasec.io/docs/blog/log4j-zero-day-update-on-cve-2021-45046/
Guest

Show your support for Open Source Security tools by starring us on GitHub.

LunaSec
Docs
Blog
Contact Us
GitHub
Search
⌘ K

All Posts

- Protestware - How node-ipc turned into malware
- Newest Vulnerability in Log4j 2.17.0 more hype than substance
- LunaDefend can help protect against Open Source vulnerabilities
- Log4Shell: RCE 0-day exploit found in log4j 2, a popular Java logging package
- Guide: How To Detect and Mitigate the Log4Shell Vulnerability (CVE-2021-44228 & CVE-2021-45046)
- Log4Shell Update: Second log4j Vulnerability Published (CVE-2021-44228 + CVE-2021-45046)
- How to Automatically Mitigate Log4Shell via a Live Patch (CVE-2021-44228 + CVE-2021-45046)
- Log4Shell Update: Severity Upgraded 3.7 to 9.0 for Second log4j Vulnerability (CVE-2021-45046)
- How to Discuss and Fix Vulnerabilities in Your Open Source Library
- Understanding Log4Shell via Exploitation and Live Patching (CVE-2021-44228 + CVE-2021-45046)

Log4Shell Update: Second log4j Vulnerability Published (CVE-2021-44228 + CVE-2021-45046)

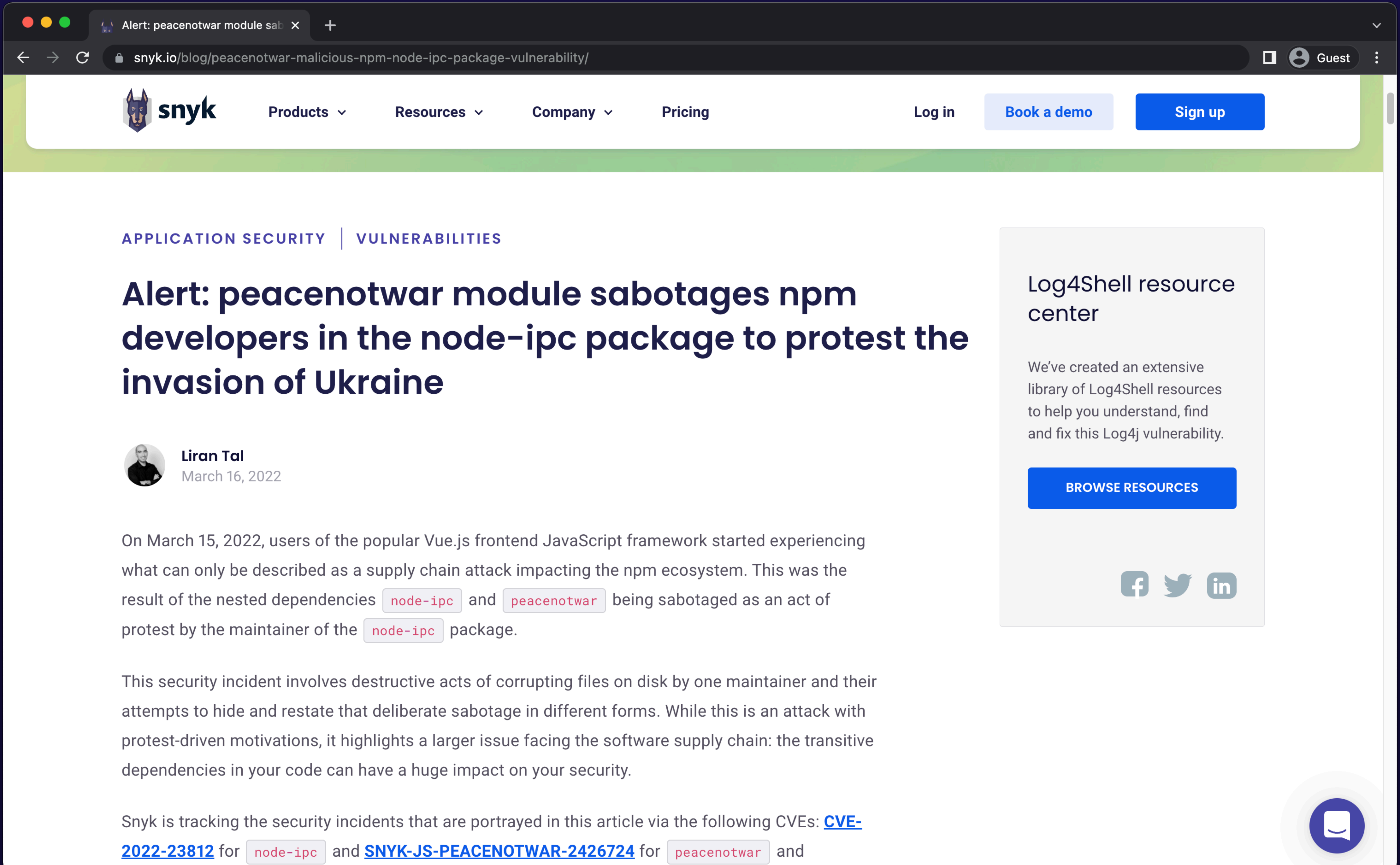
December 19, 2021 · 8 min read

Free Wortley
CEO at LunaSec

Chris Thompson
Developer at Lunasec

Forrest Allison
Developer at LunaSec

- Conditions for the vulnerability
- The new CVE is difficult to understand
- Context on CVE-2021-45046
- Testing previous mitigations
- Our Findings
  - Issues when using `log4j2.formatMsgNoLookups` (>=2.10.0)
  - Setting `%m{nolookups}` is still vulnerable (>=2.7.0)
  - Notes on the Denial-of-Service in 2.15.0
- Stay Updated
- Additional Information
  - Limited Offer: Free Security Assistance
- Updates


Alert: peacenotwar module sab
snyk.io/blog/peacenotwar-malicious-npm-node-ipc-package-vulnerability/
Guest
snyk
Products
Resources
Company
Pricing
Log in
Book a demo
Sign up

APPLICATION SECURITY | VULNERABILITIES

Alert: peacenotwar module sabotages npm developers in the node-ipc package to protest the invasion of Ukraine

Liran Tal
March 16, 2022

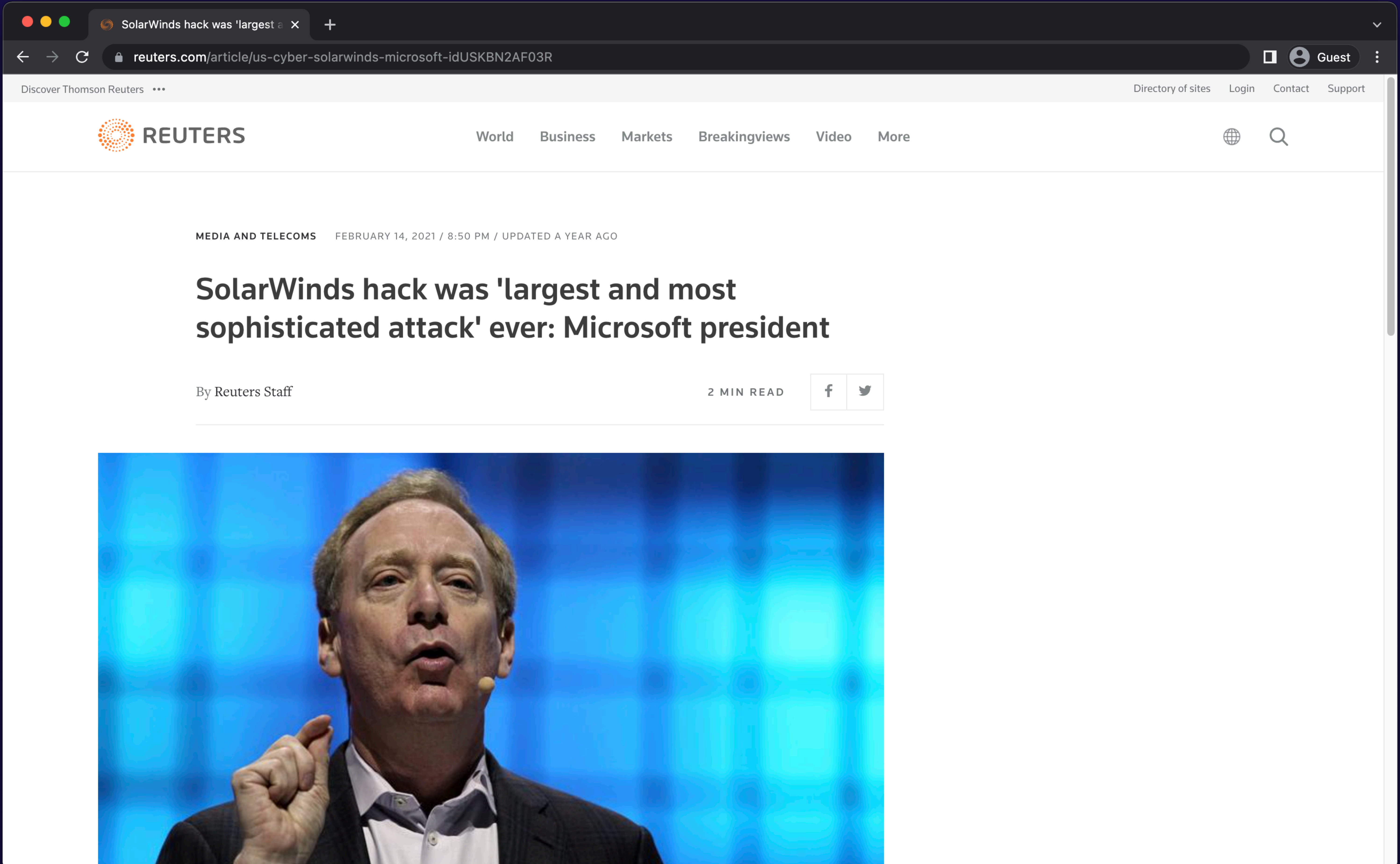
On March 15, 2022, users of the popular Vue.js frontend JavaScript framework started experiencing what can only be described as a supply chain attack impacting the npm ecosystem. This was the result of the nested dependencies `node-ipc` and `peacenotwar` being sabotaged as an act of protest by the maintainer of the `node-ipc` package.

This security incident involves destructive acts of corrupting files on disk by one maintainer and their attempts to hide and restate that deliberate sabotage in different forms. While this is an attack with protest-driven motivations, it highlights a larger issue facing the software supply chain: the transitive dependencies in your code can have a huge impact on your security.

Snyk is tracking the security incidents that are portrayed in this article via the following CVEs: CVE-2022-23812 for `node-ipc` and SNYK-JS-PEACENOTWAR-2426724 for `peacenotwar` and

Log4Shell resource center

We've created an extensive library of Log4Shell resources to help you understand, find and fix this Log4j vulnerability.

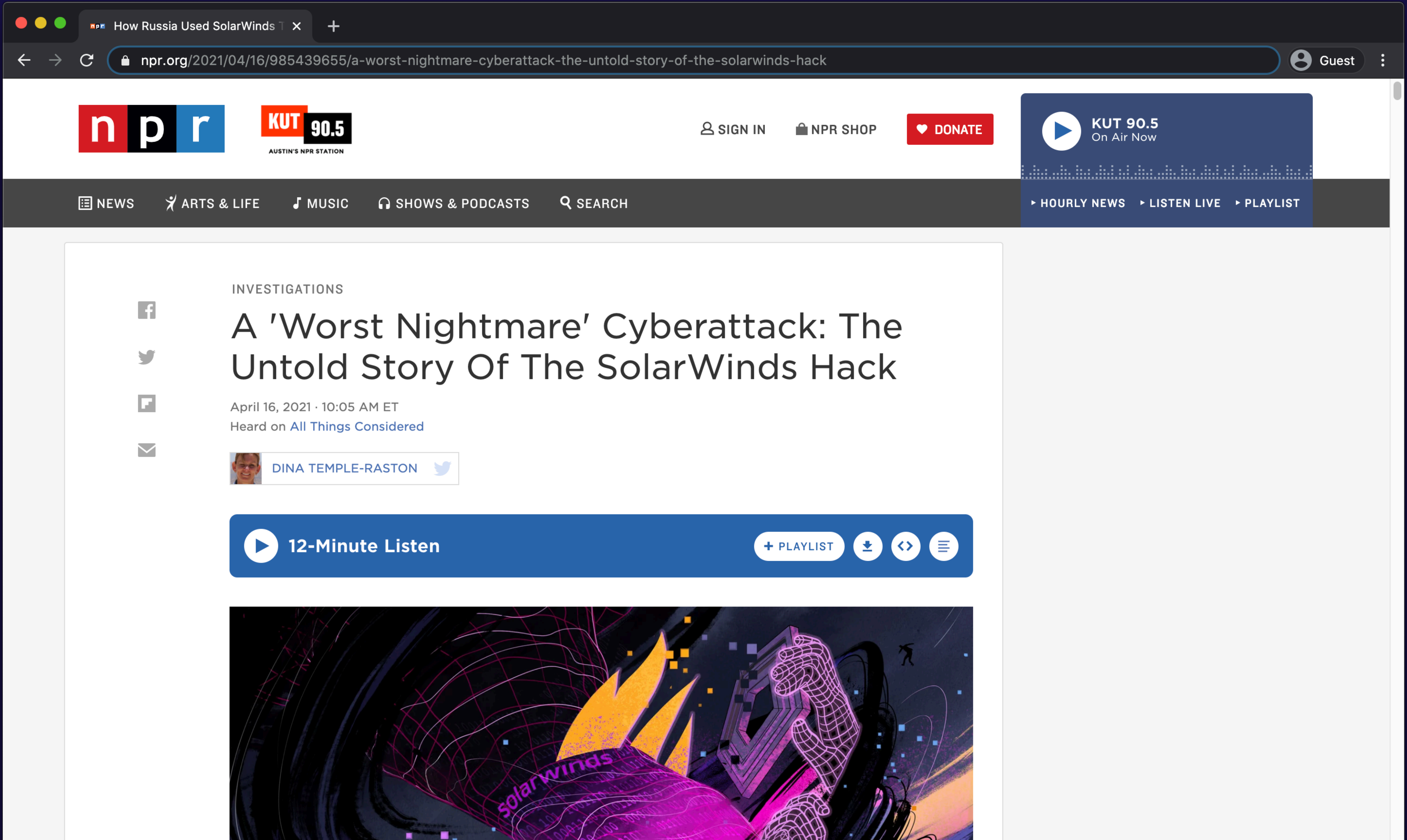


MEDIA AND TELECOMS FEBRUARY 14, 2021 / 8:50 PM / UPDATED A YEAR AGO

SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president

By Reuters Staff

2 MIN READ



How Russia Used SolarWinds T

npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

Guest

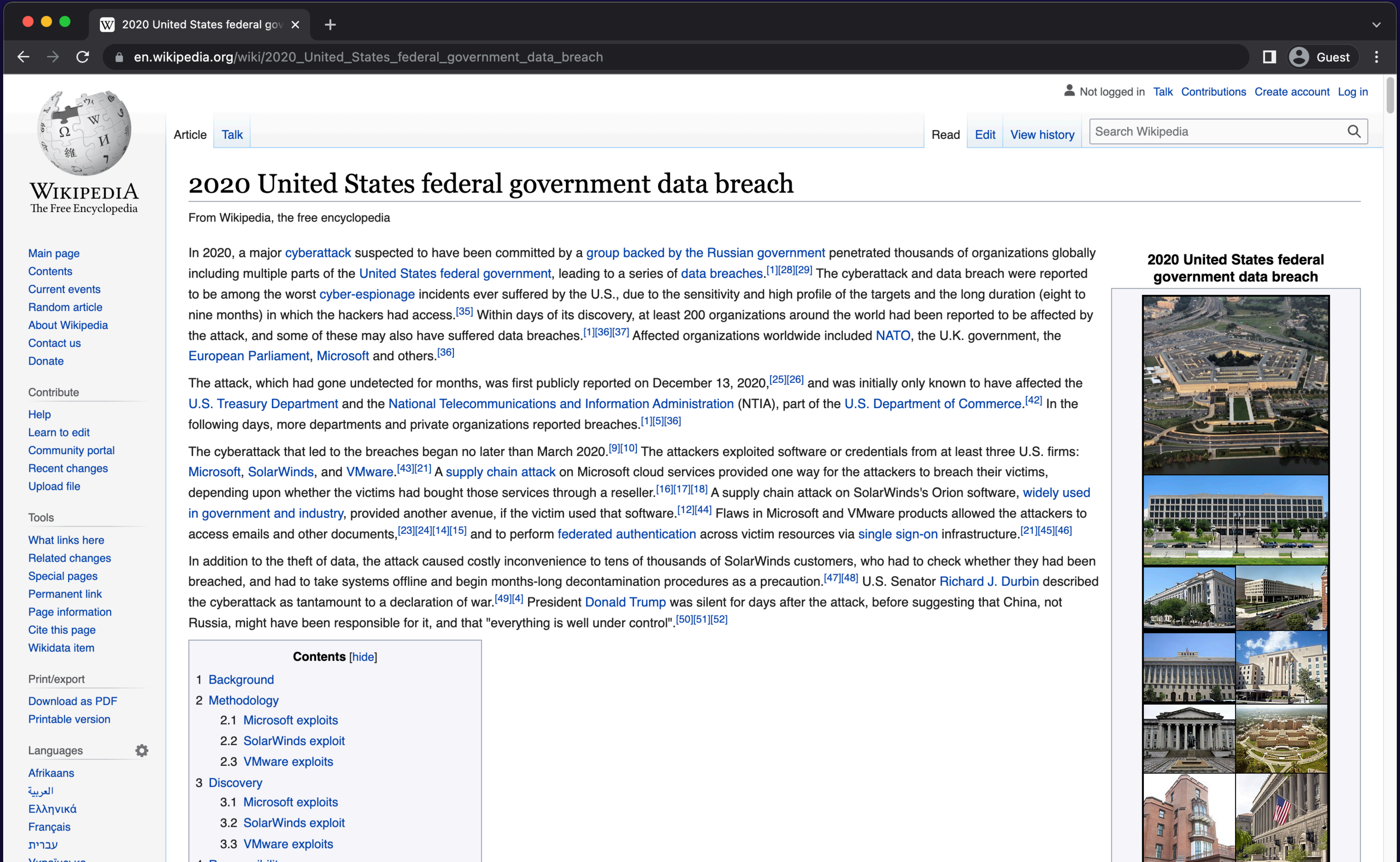
INVESTIGATIONS

A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack

April 16, 2021 · 10:05 AM ET

Heard on All Things Considered

DINA TEMPLE-RASTON



2020 United States federal gov
en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach
Guest
Not logged in Talk Contributions Create account Log in
Wikipedia
The Free Encyclopedia
Article Talk
Read Edit View history
Search Wikipedia

Main page
Contents
Current events
Random article
About Wikipedia
Contact us
Donate

Contribute
Help
Learn to edit
Community portal
Recent changes
Upload file

Tools
What links here
Related changes
Special pages
Permanent link
Page information
Cite this page
Wikidata item

Print/export
Download as PDF
Printable version

Languages
Afrikaans
العربية
Ελληνικά
Français
עברית

2020 United States federal government data breach

From Wikipedia, the free encyclopedia

In 2020, a major cyberattack suspected to have been committed by a group backed by the Russian government penetrated thousands of organizations globally including multiple parts of the United States federal government, leading to a series of data breaches.[1][28][29] The cyberattack and data breach were reported to be among the worst cyber-espionage incidents ever suffered by the U.S., due to the sensitivity and high profile of the targets and the long duration (eight to nine months) in which the hackers had access.[35] Within days of its discovery, at least 200 organizations around the world had been reported to be affected by the attack, and some of these may also have suffered data breaches.[1][36][37] Affected organizations worldwide included NATO, the U.K. government, the European Parliament, Microsoft and others.[36]

The attack, which had gone undetected for months, was first publicly reported on December 13, 2020,[25][26] and was initially only known to have affected the U.S. Treasury Department and the National Telecommunications and Information Administration (NTIA), part of the U.S. Department of Commerce.[42] In the following days, more departments and private organizations reported breaches.[1][5][36]

The cyberattack that led to the breaches began no later than March 2020.[9][10] The attackers exploited software or credentials from at least three U.S. firms: Microsoft, SolarWinds, and VMware.[43][21] A supply chain attack on Microsoft cloud services provided one way for the attackers to breach their victims, depending upon whether the victims had bought those services through a reseller.[16][17][18] A supply chain attack on SolarWinds's Orion software, widely used in government and industry, provided another avenue, if the victim used that software.[12][44] Flaws in Microsoft and VMware products allowed the attackers to access emails and other documents,[23][24][14][15] and to perform federated authentication across victim resources via single sign-on infrastructure.[21][45][46]

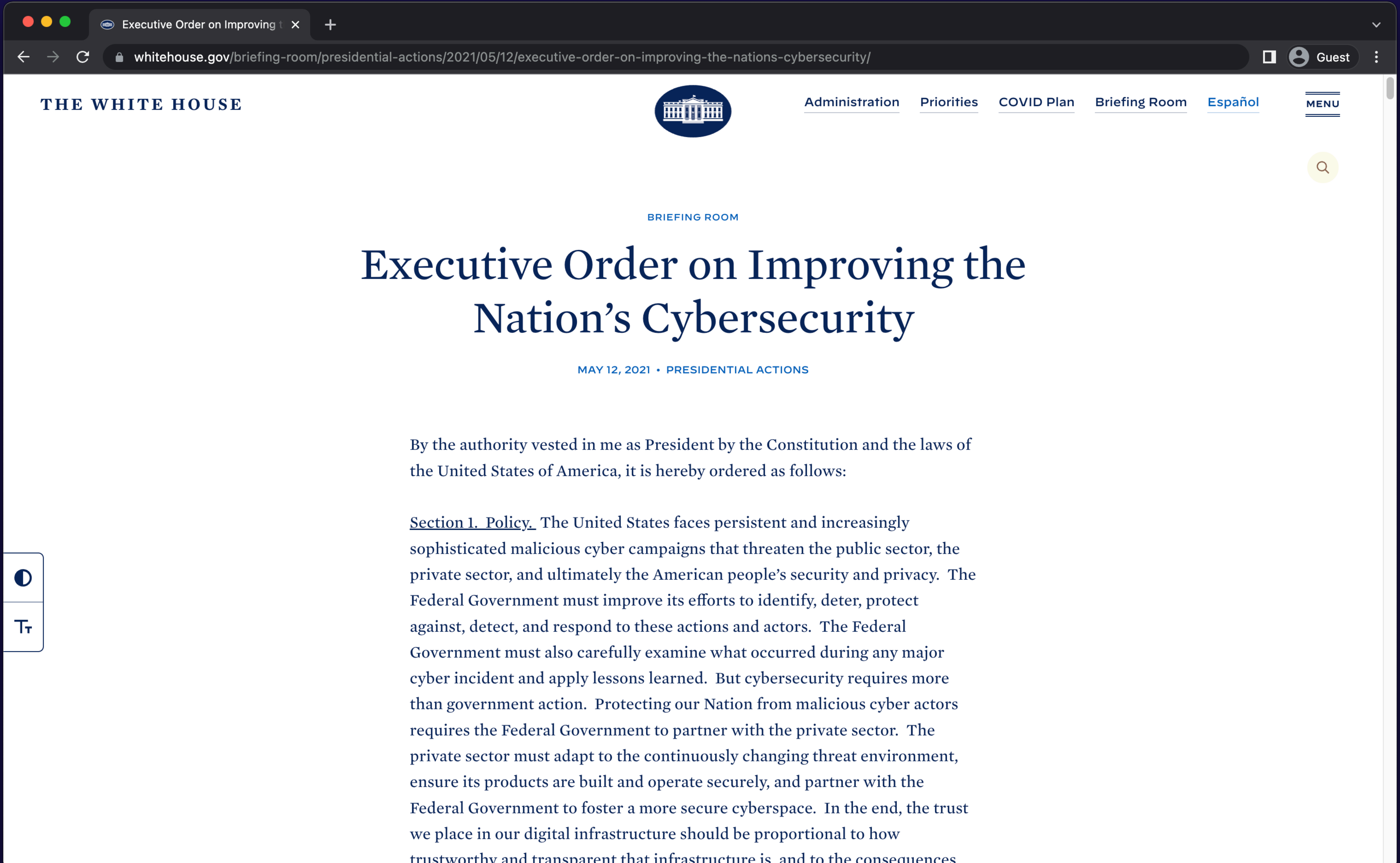
In addition to the theft of data, the attack caused costly inconvenience to tens of thousands of SolarWinds customers, who had to check whether they had been breached, and had to take systems offline and begin months-long decontamination procedures as a precaution.[47][48] U.S. Senator Richard J. Durbin described the cyberattack as tantamount to a declaration of war.[49][4] President Donald Trump was silent for days after the attack, before suggesting that China, not Russia, might have been responsible for it, and that "everything is well under control".[50][51][52]

2020 United States federal government data breach

Contents [hide]

1 Background
2 Methodology
2.1 Microsoft exploits
2.2 SolarWinds exploit
2.3 VMware exploits
3 Discovery
3.1 Microsoft exploits
3.2 SolarWinds exploit
3.3 VMware exploits

But the main reason...


Executive Order on Improving t
whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
Guest
THE WHITE HOUSE
Administration
Priorities
COVID Plan
Briefing Room
Español
MENU

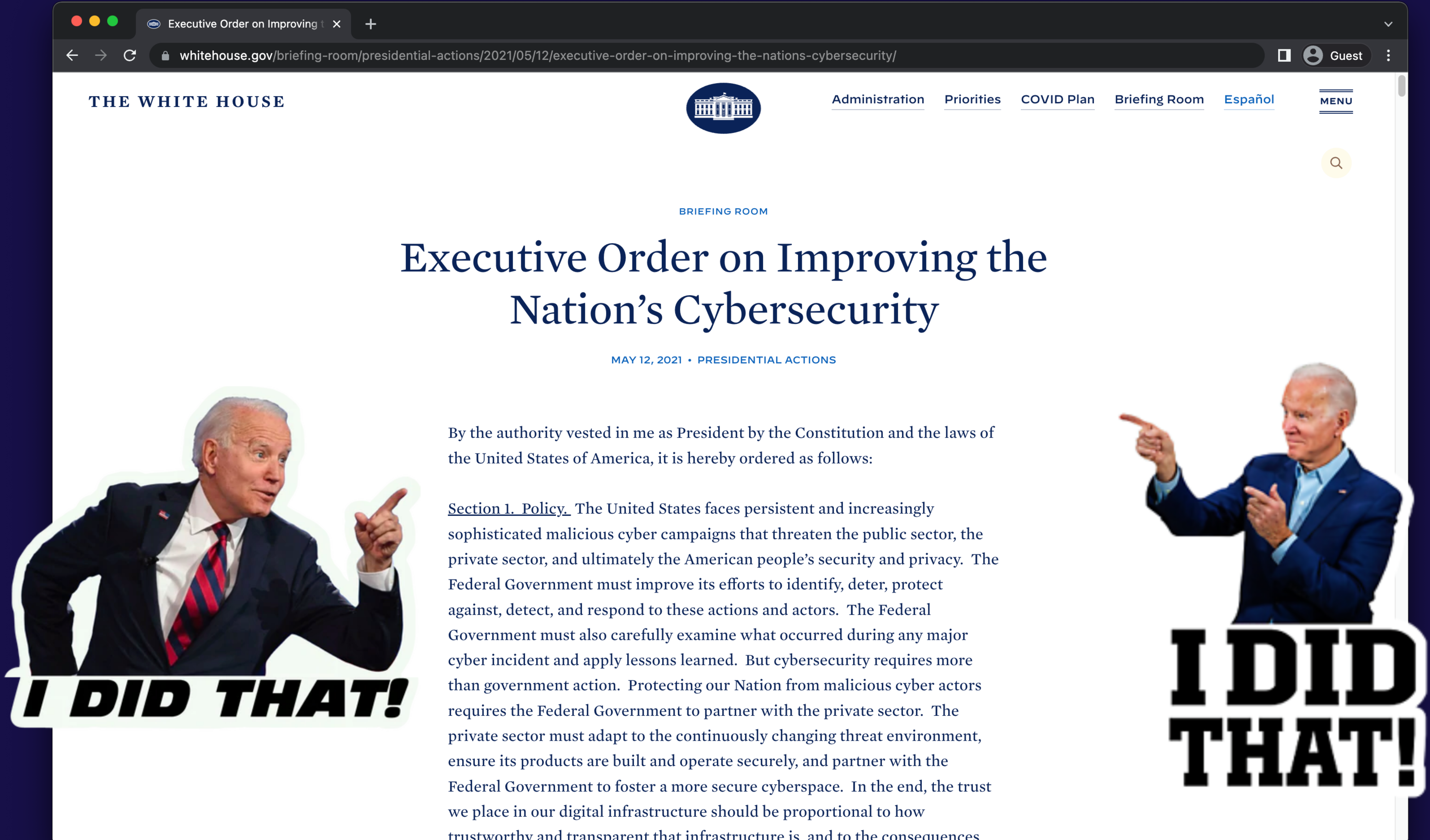
BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences



Executive Order on Improving t
whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
Guest
THE WHITE HOUSE
Administration
Priorities
COVID Plan
Briefing Room
Español
MENU
I DID THAT!
I DID THAT!

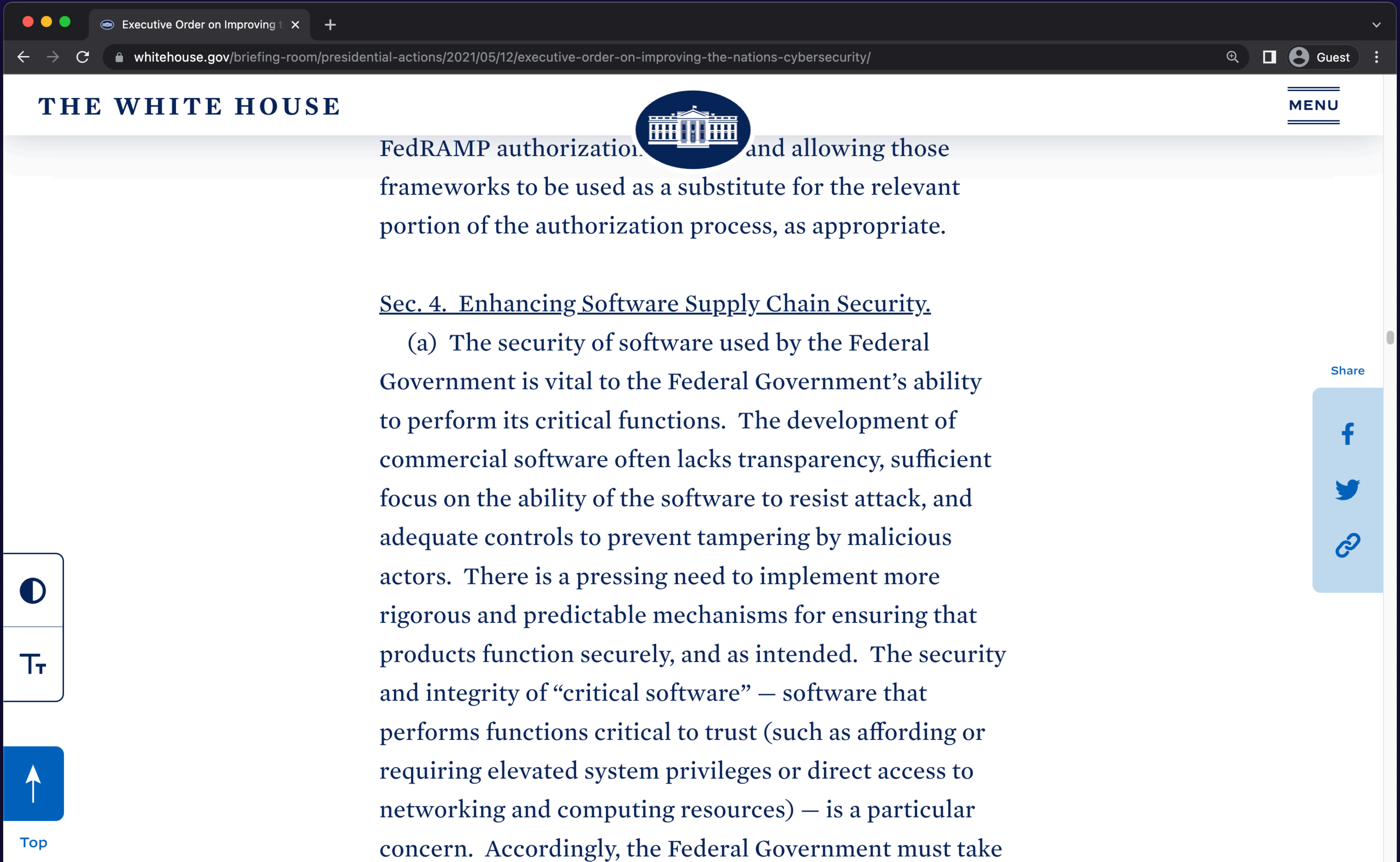
BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences


Executive Order on Improving t
whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
Guest
THE WHITE HOUSE
MENU
Share
Top

FedRAMP authorizatio and allowing those frameworks to be used as a substitute for the relevant portion of the authorization process, as appropriate.

Sec. 4. Enhancing Software Supply Chain Security.

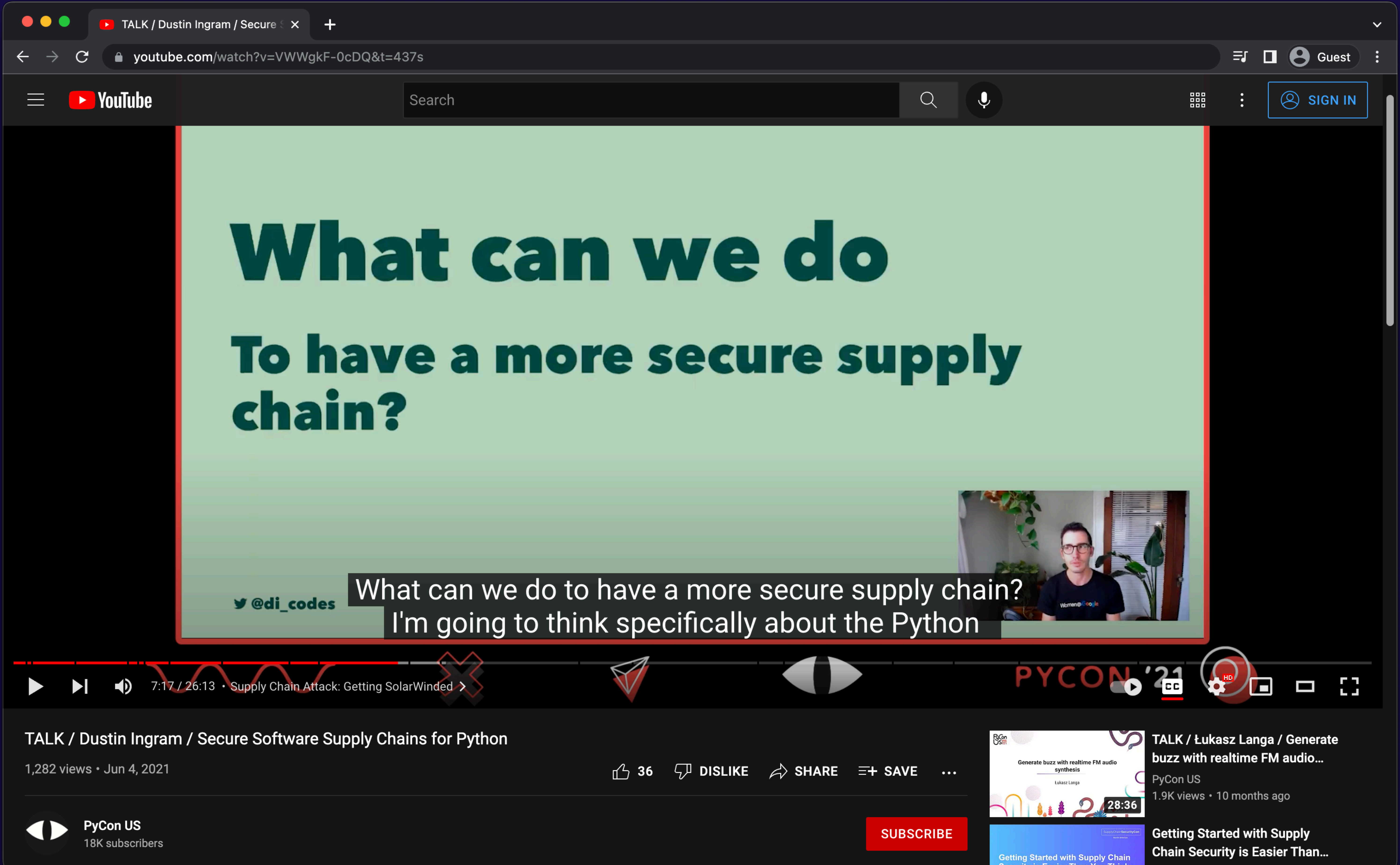
(a) The security of software used by the Federal Government is vital to the Federal Government's ability to perform its critical functions. The development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors. There is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended. The security and integrity of "critical software" — software that performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resources) — is a particular concern. Accordingly, the Federal Government must take

Part 2:

Parts of the Secure Software Supply Chain

Part 3:

How can we use open-source software safely?



TALK / Dustin Ingram / Secure

youtube.com/watch?v=VWWgkF-0cDQ&t=437s

Guest

Search

SIGN IN

What can we do

To have a more secure supply chain?

@di_codes

What can we do to have a more secure supply chain?
I'm going to think specifically about the Python

7:17 / 26:13 • Supply Chain Attack: Getting SolarWinded

TALK / Dustin Ingram / Secure Software Supply Chains for Python

1,282 views • Jun 4, 2021

36 DISLIKE SHARE SAVE

PyCon US
18K subscribers

SUBSCRIBE

TALK / Łukasz Langa / Generate buzz with realtime FM audio...
PyCon US
1.9K views • 10 months ago
28:36

Getting Started with Supply Chain Security is Easier Than...

PYCON '21
Generate buzz with realtime FM audio synthesis
Łukasz Langa
Getting Started with Supply Chain

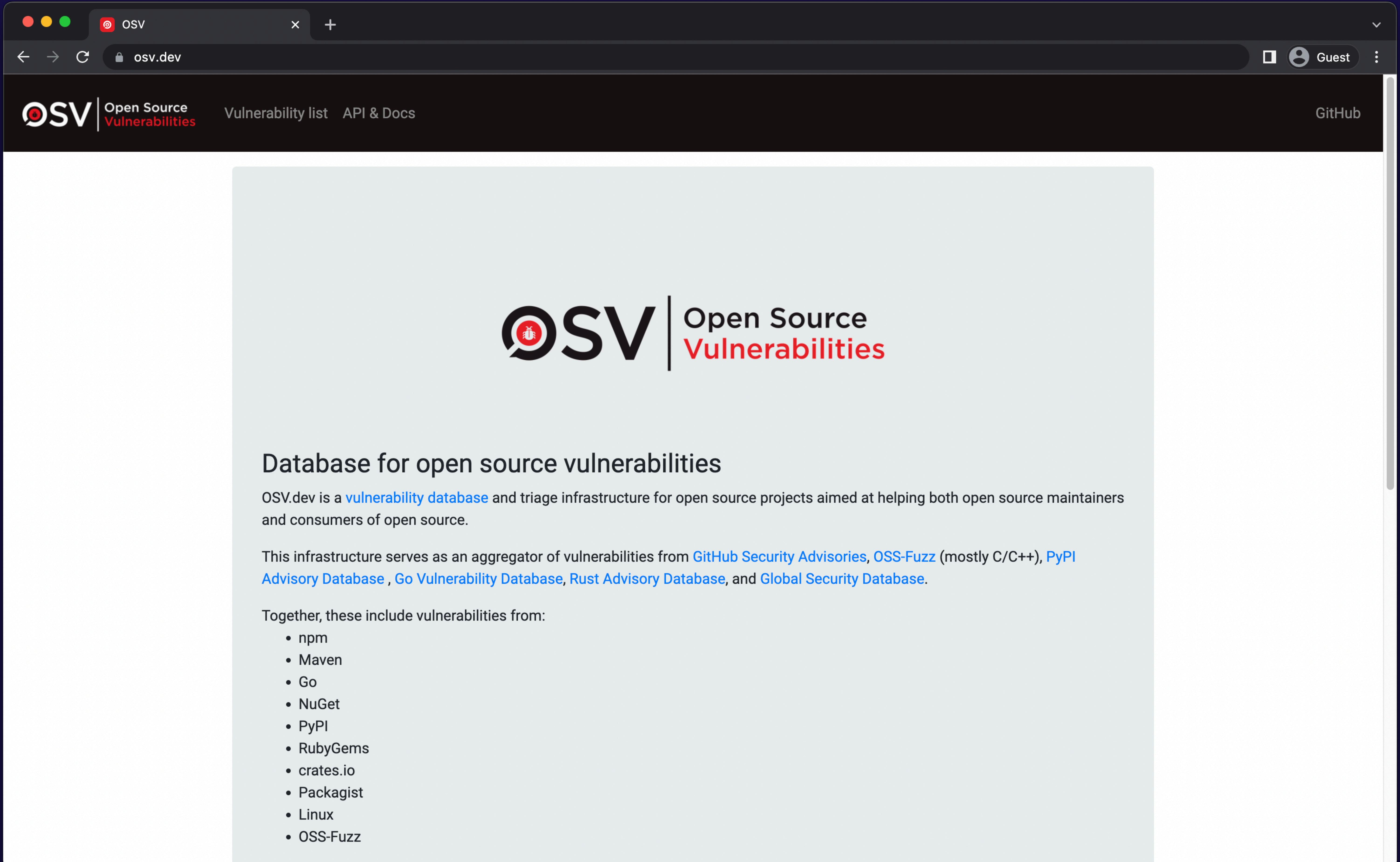
What we can do (circa 2021):

- HTTPS everywhere
- Lockfiles & compiled dependencies
- Vulnerability notifications
- TUF, namespaces, etc

What *else* can we do to fix this?

New!

Community advisory databases



OSV
osv.dev
Guest
OSV Open Source Vulnerabilities
Vulnerability list
API & Docs
GitHub
OSV Open Source Vulnerabilities

Database for open source vulnerabilities

OSV.dev is a vulnerability database and triage infrastructure for open source projects aimed at helping both open source maintainers and consumers of open source.

This infrastructure serves as an aggregator of vulnerabilities from GitHub Security Advisories, OSS-Fuzz (mostly C/C++), PyPI Advisory Database , Go Vulnerability Database, Rust Advisory Database, and Global Security Database.

Together, these include vulnerabilities from:

- npm
- Maven
- Go
- NuGet
- PyPI
- RubyGems
- crates.io
- Packagist
- Linux
- OSS-Fuzz

Community advisory databases

https://github.com/pypa/advisory-database

New!

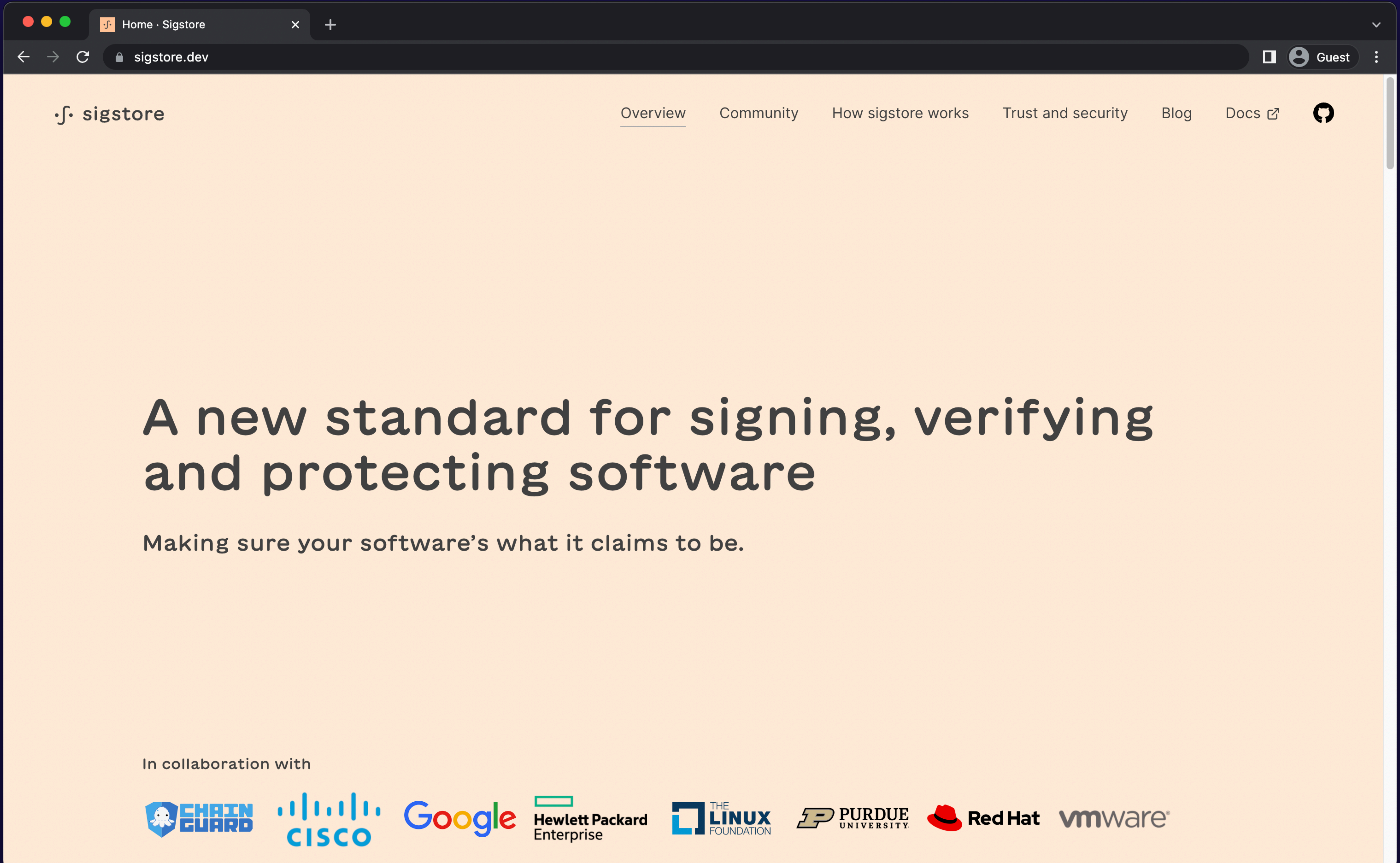
Vulnerability auditing software

Use vulnerability auditing software:

- Python: `pip-audit`
- Go: `vulncheck`
- Rust: `cargo-audit`
- Ruby: `bundler-audit`

Improvement:

Artifact Signing



A new standard for signing, verifying and protecting software

Making sure your software's what it claims to be.

In collaboration with

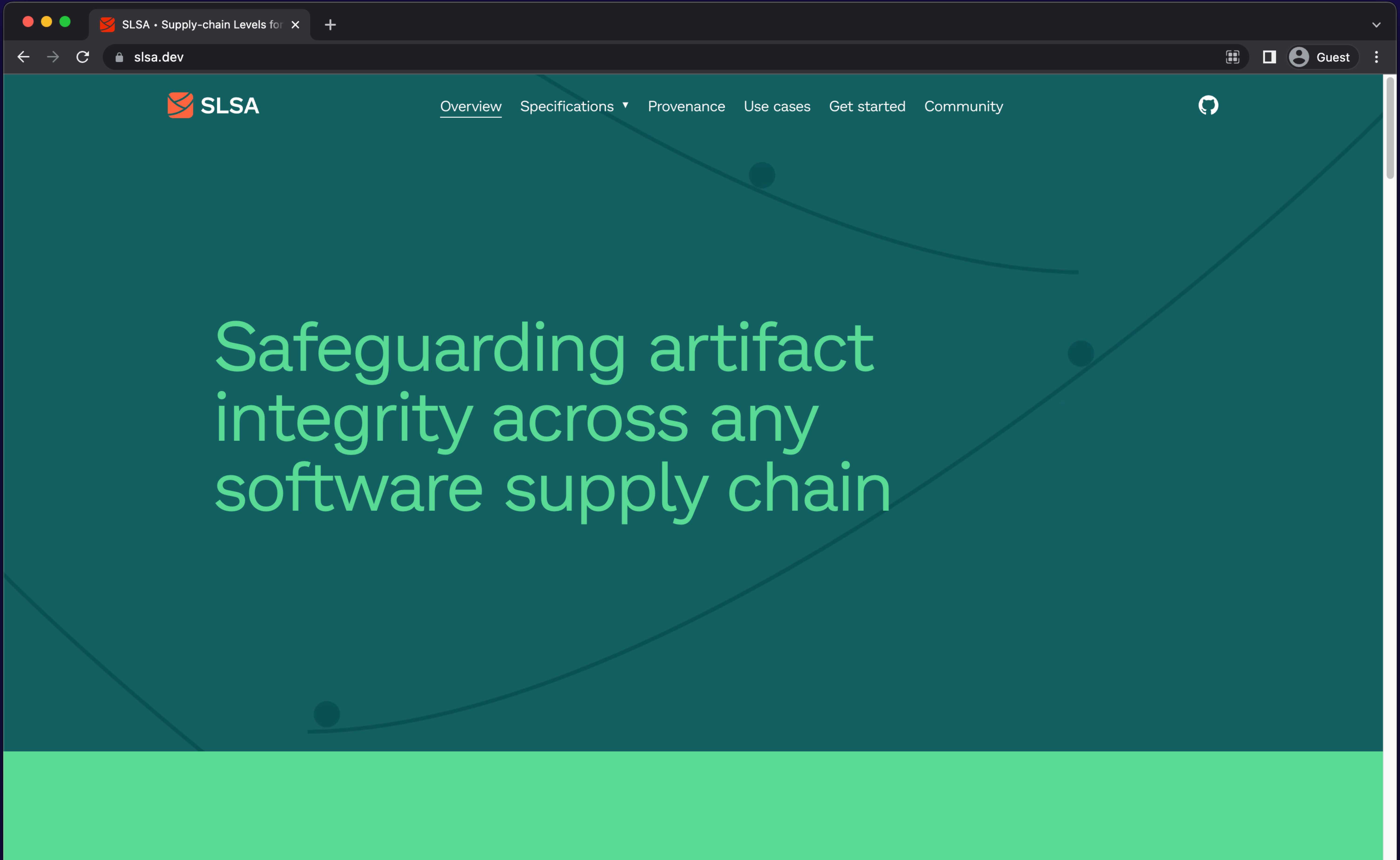
Understanding sigstore

- Ephemeral keys
- Certificate authority
- Transparency log
- Timestamping service
- OpenID Connect

sigstore-python

Improvement:

Better, more secure build infrastructure



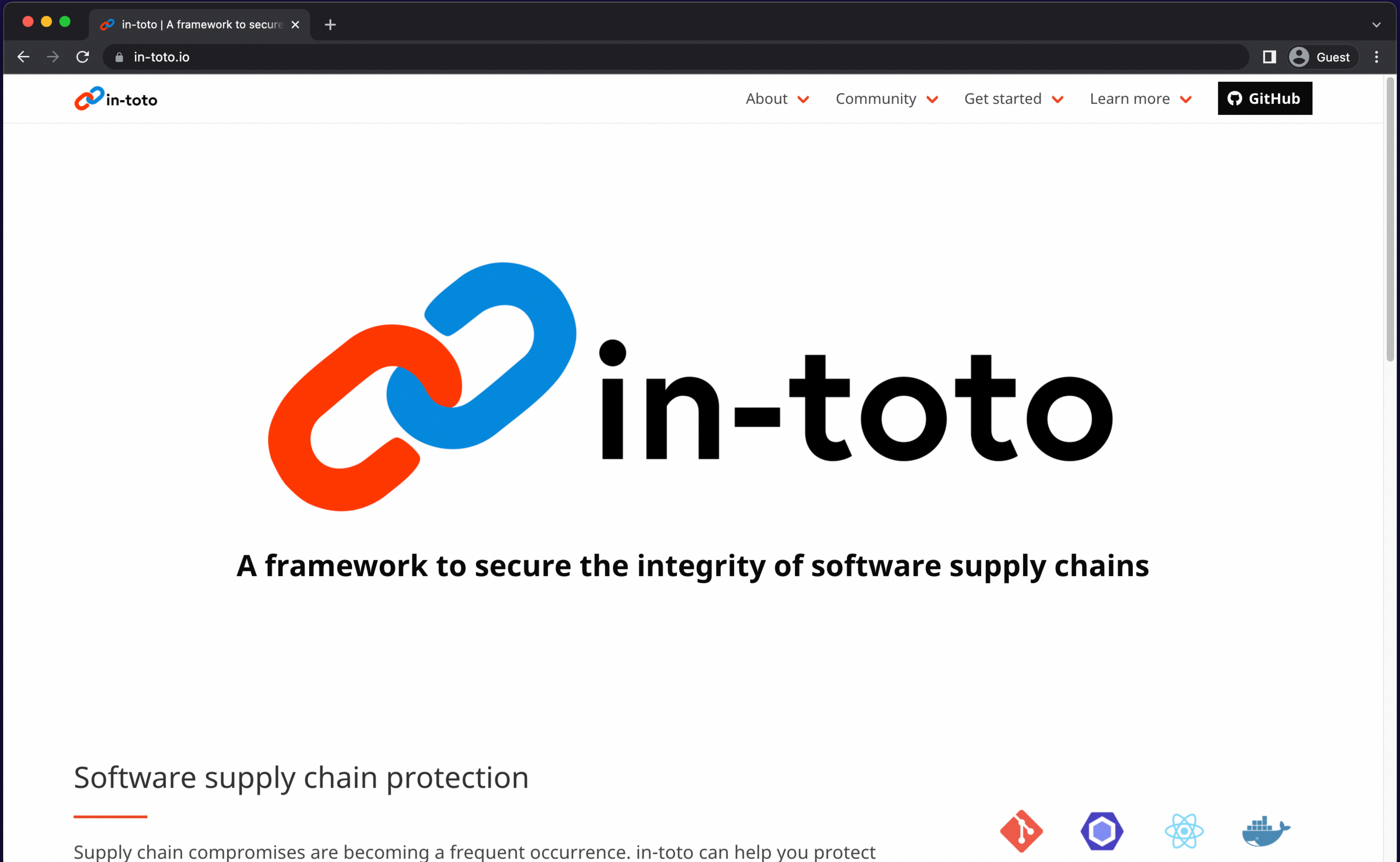
Safeguarding artifact integrity across any software supply chain

Understanding SLSA ('salsa')

- Security framework
- Checklist of standards and controls
- A series of levels

Improvement:

Attestations



A framework to secure the integrity of software supply chains

Software supply chain protection

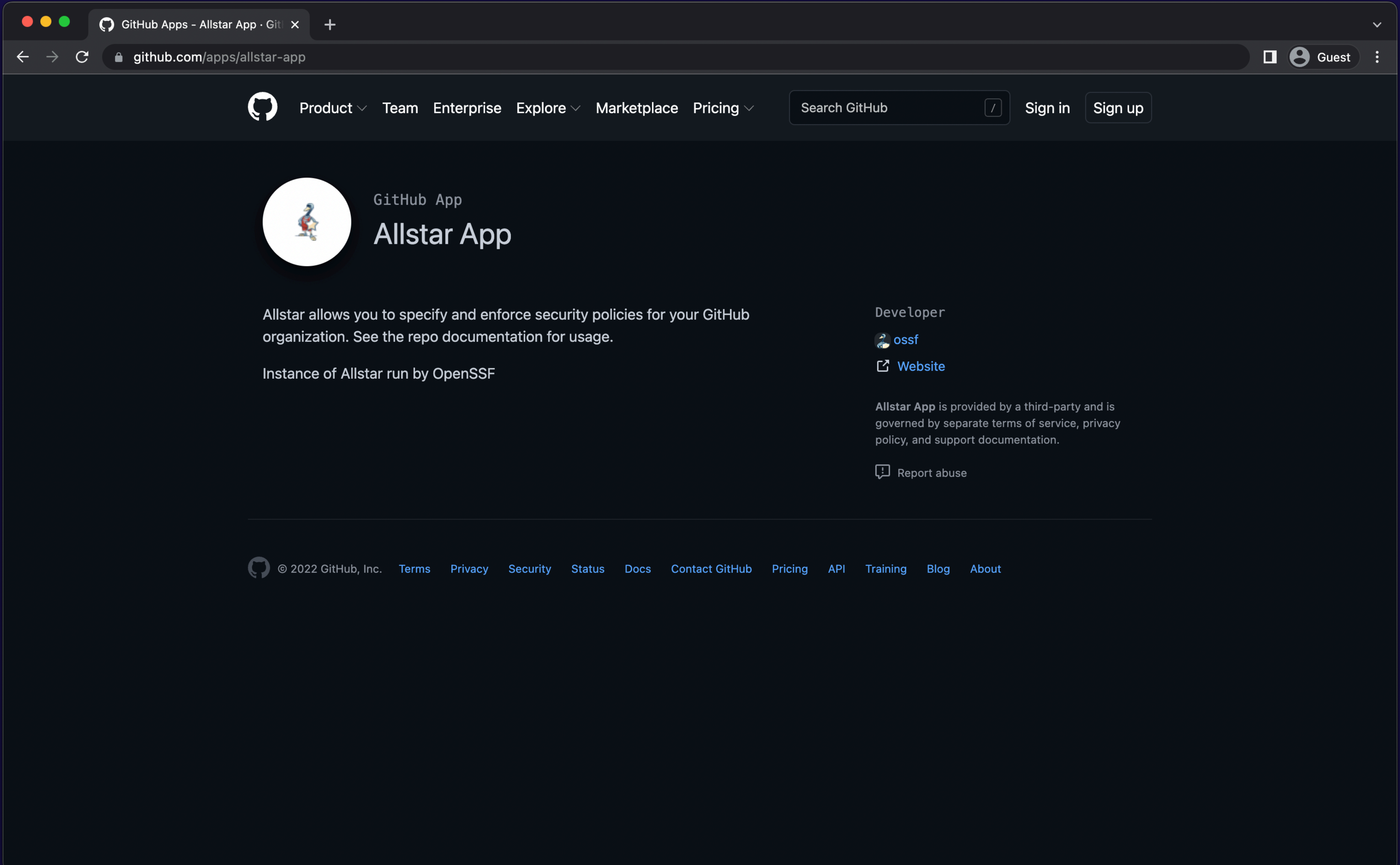
Supply chain compromises are becoming a frequent occurrence. in-toto can help you protect

Understanding in-toto

- A universal standard
- For all ecosystems
- Ensuring integrity of an artifact
- Proof of what was done at each step

Improvement:

Enforcing security policies for source control



GitHub App

Allstar App

Allstar allows you to specify and enforce security policies for your GitHub organization. See the repo documentation for usage.

Instance of Allstar run by OpenSSF

Developer

ossf

Website

Allstar App is provided by a third-party and is governed by separate terms of service, privacy policy, and support documentation.

Report abuse

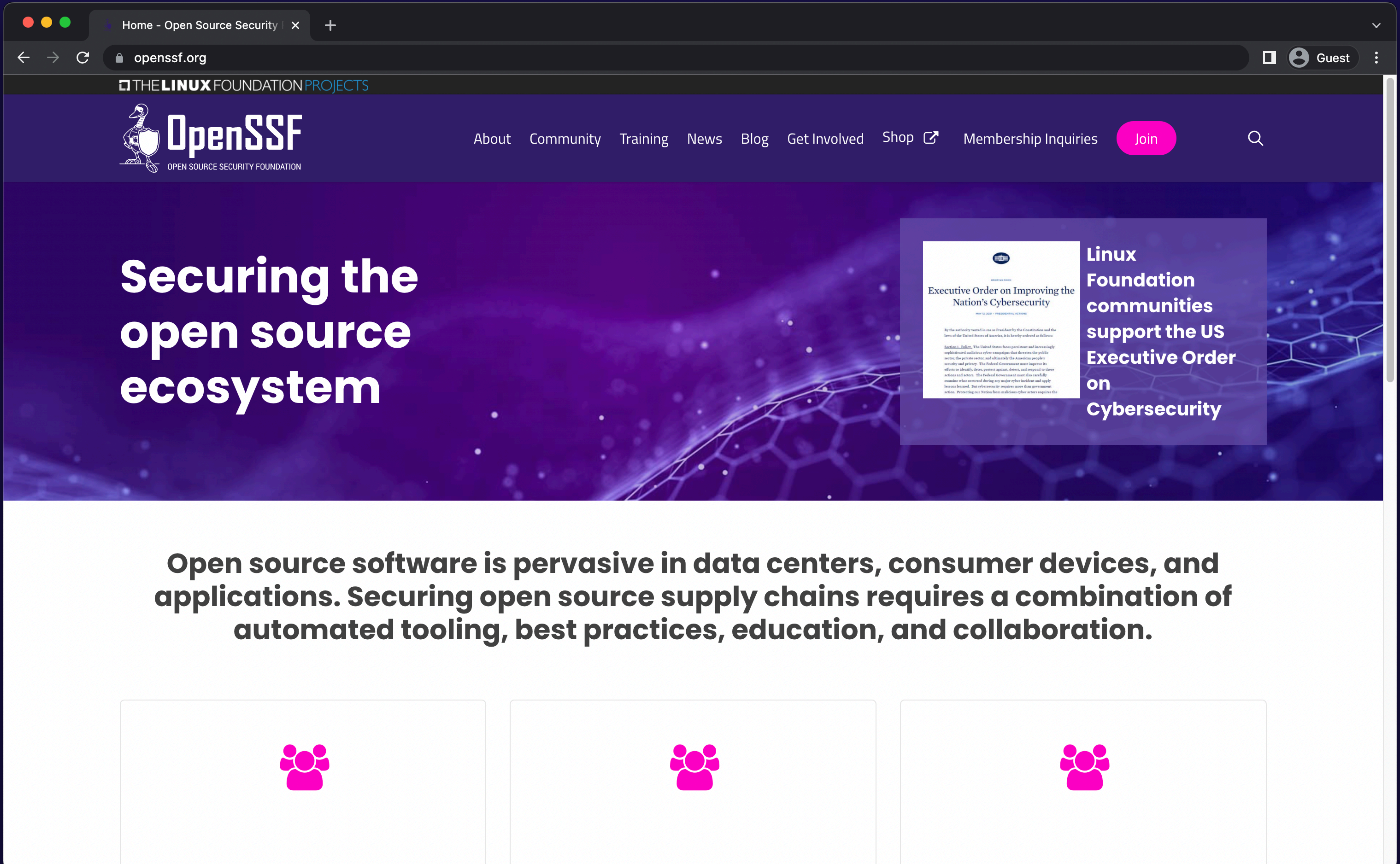
© 2022 GitHub, Inc.

Understanding Allstar

- A GitHub app
- Enforces best practices
- Allows you to set policy
- Across an entire organization

Improvement:

Vendor neutral collaboration



Securing the open source ecosystem

Executive Order on Improving the Nation's Cybersecurity

Linux Foundation communities support the US Executive Order on Cybersecurity

Open source software is pervasive in data centers, consumer devices, and applications. Securing open source supply chains requires a combination of automated tooling, best practices, education, and collaboration.

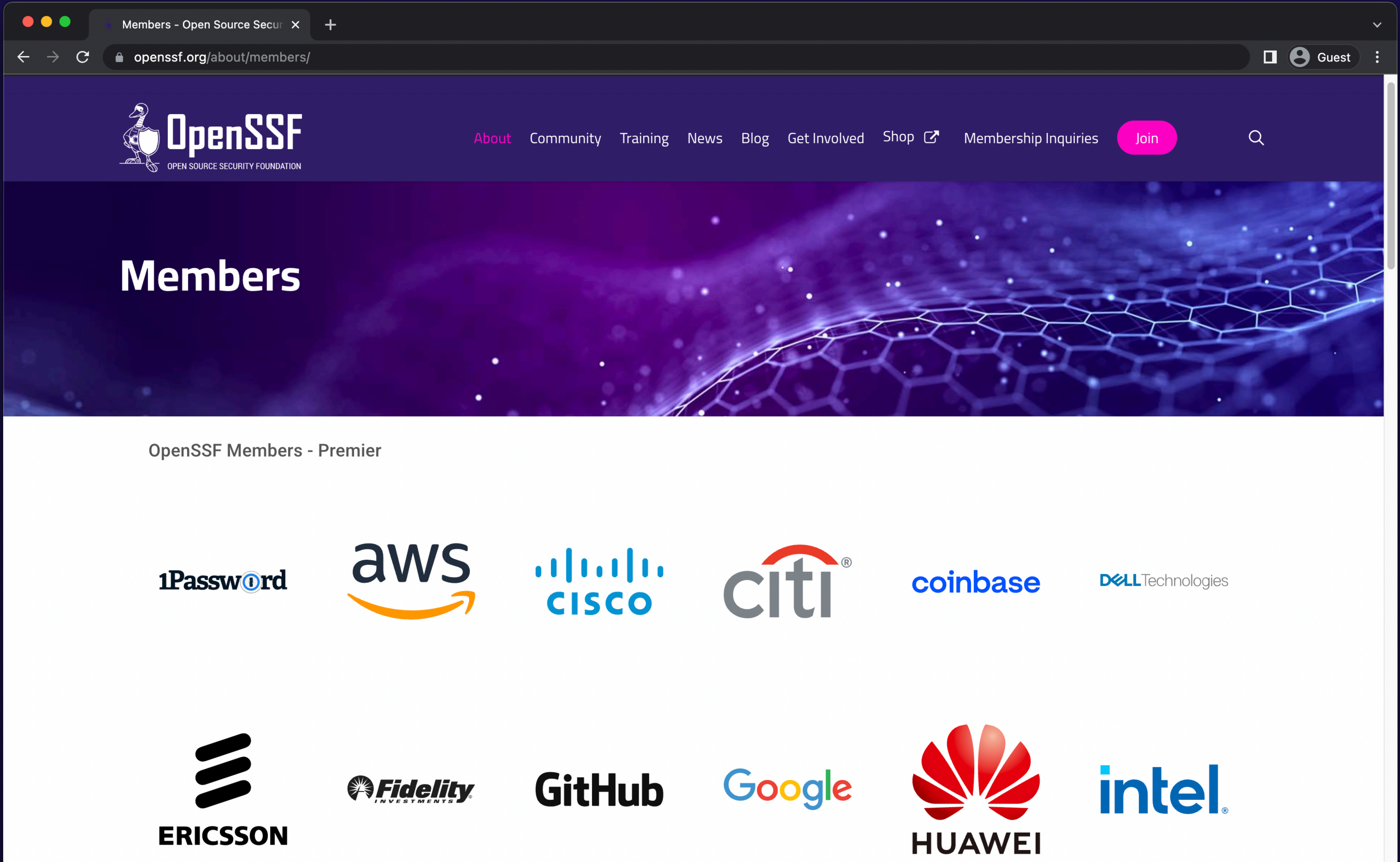
Improvement

New features for PyPI

What *else* can we do to fix this?

Improvement:

More funding for projects


Members - Open Source Secur
openssf.org/about/members/
Guest
OpenSSF
OPEN SOURCE SECURITY FOUNDATION
About
Community
Training
News
Blog
Get Involved
Shop
Membership Inquiries
Join

Members

OpenSSF Members - Premier

1Password | aws | cisco | citi | coinbase | DELL Technologies

ERICSSON | Fidelity INVESTMENTS | GitHub | Google | HUAWEI | intel

Improvement:

More users and contributors!

Predictions

My predictions for the next year

Shoutouts

- William Woodruff & Alex Cameron @ Trail of Bits
- PyCon Staff

Thanks!

🐦 **@di_codes**