



# Reviewing NuGet Packages security easily using OpenSSF Scorecard

Niels Tanis  
Sr. Principal Security Researcher





# Who am I?

- Niels Tanis
- Sr. Principal Security Researcher
  - Background .NET Development, Pentesting/ethical hacking, and software security consultancy
  - Research on static analysis for .NET apps
  - Enjoying Rust!
- Microsoft MVP – Developer Technologies

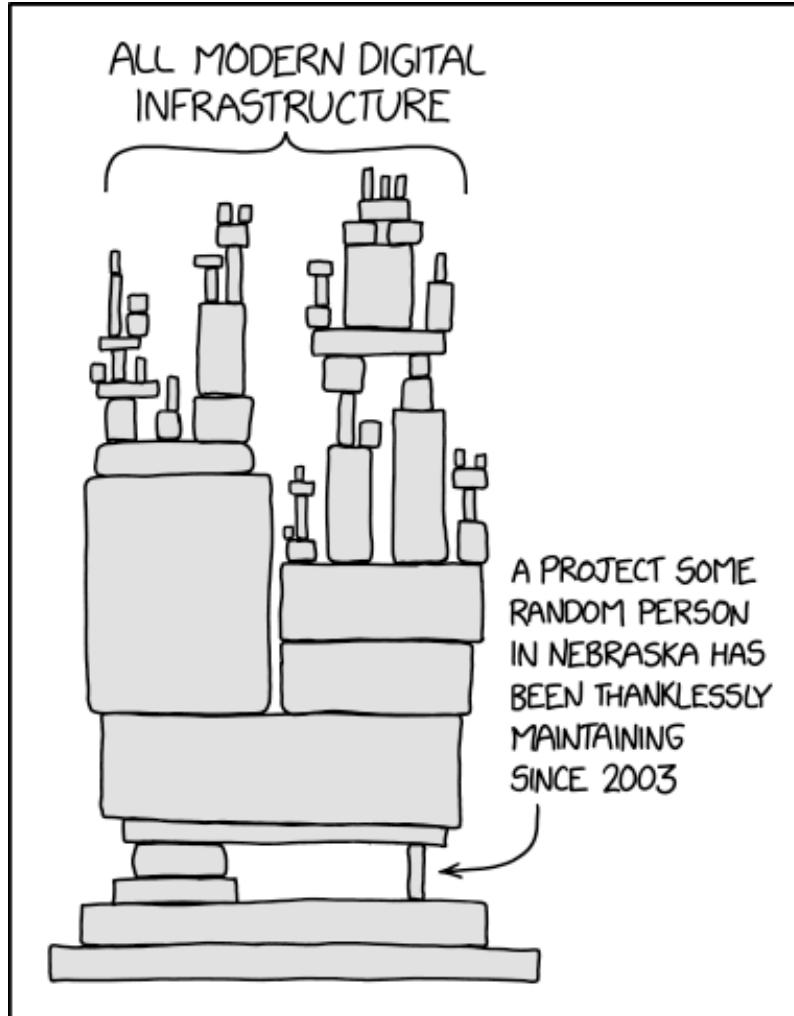
**VERACODE**



 @nielstanis@infosec.exchange

# Modern Application Architecture

## XKCD 2347





# Agenda

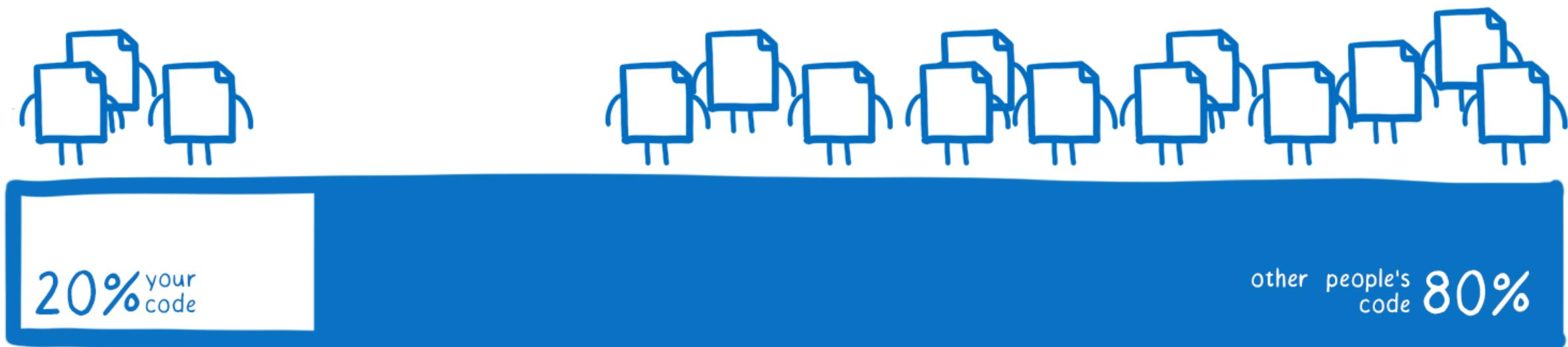
- Risks in 3<sup>rd</sup> NuGet Package
- OpenSSF Scorecard
- New & Improved
- Conclusion - Q&A



@nielstanis@infosec.exchange



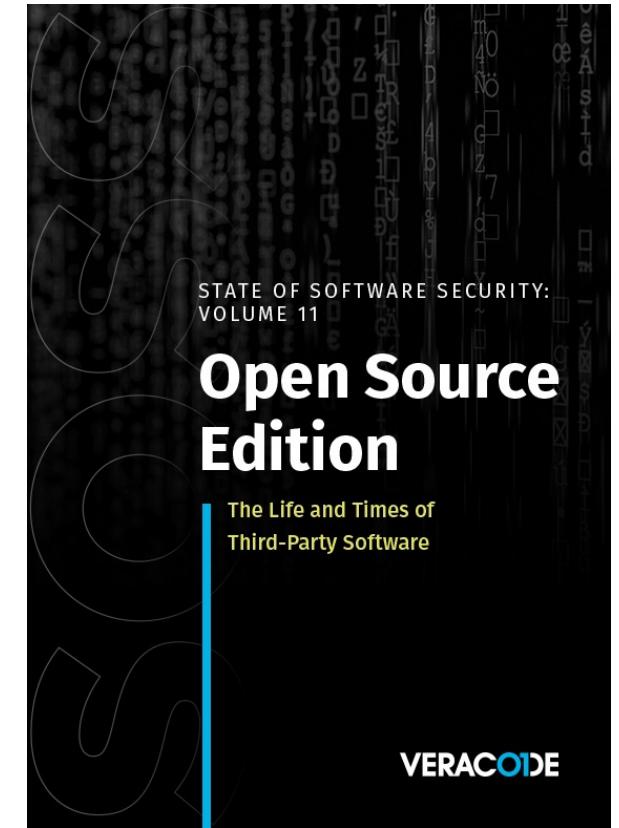
# Average codebase composition





# State of Software Security v11

*“Despite this dynamic landscape, 79 percent of the time, developers never update third-party libraries after including them in a codebase.”*





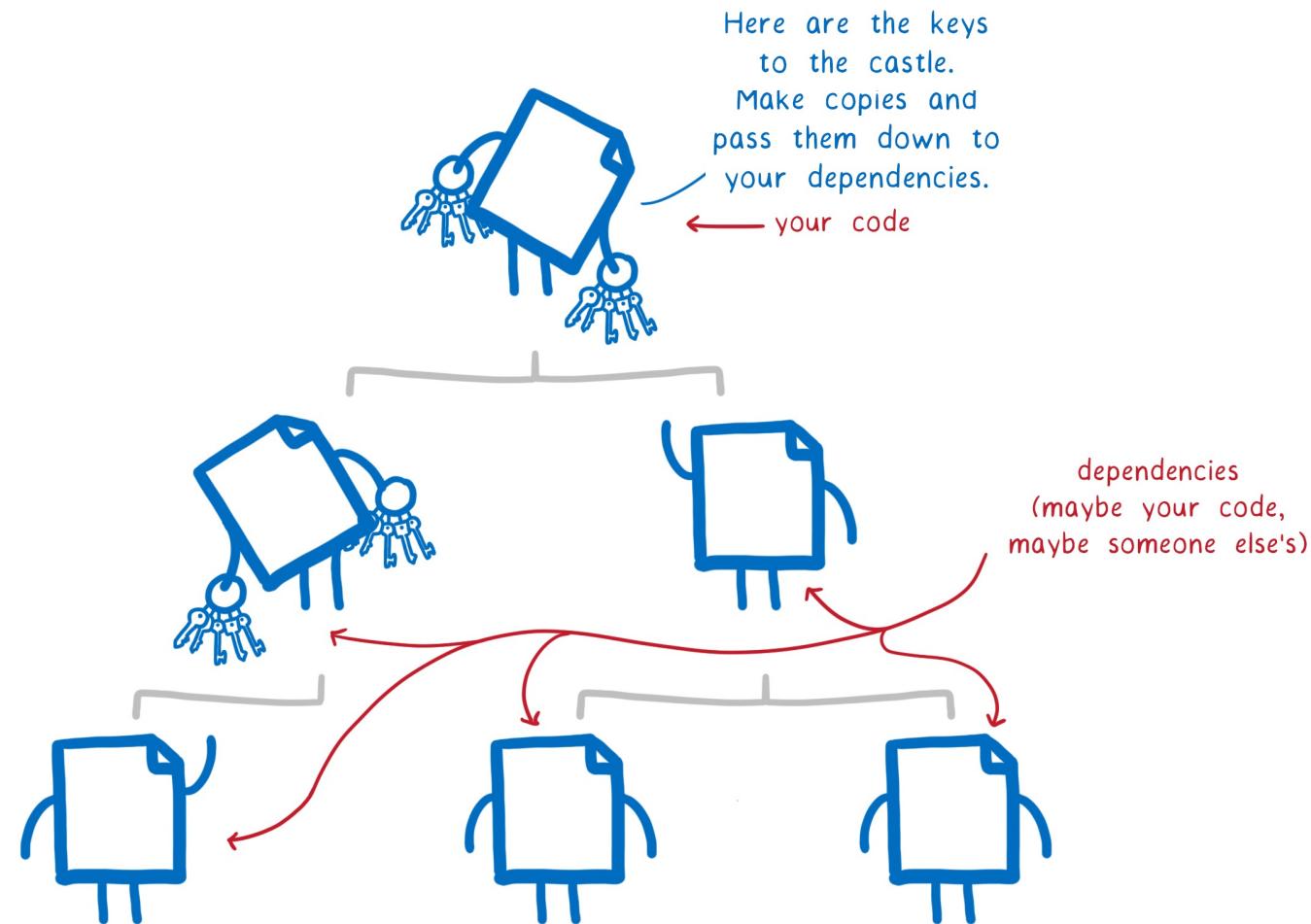
# State of Log4j - 2 years later

- Analysed our data August-November 2023
  - Total set of almost 39K unique applications scanned
- 2.8% run version vulnerable to Log4Shell
- 3.8% run version patched but vulnerable to other CVE
- 32% rely on a version that's end-of-life and have no support for any patches.



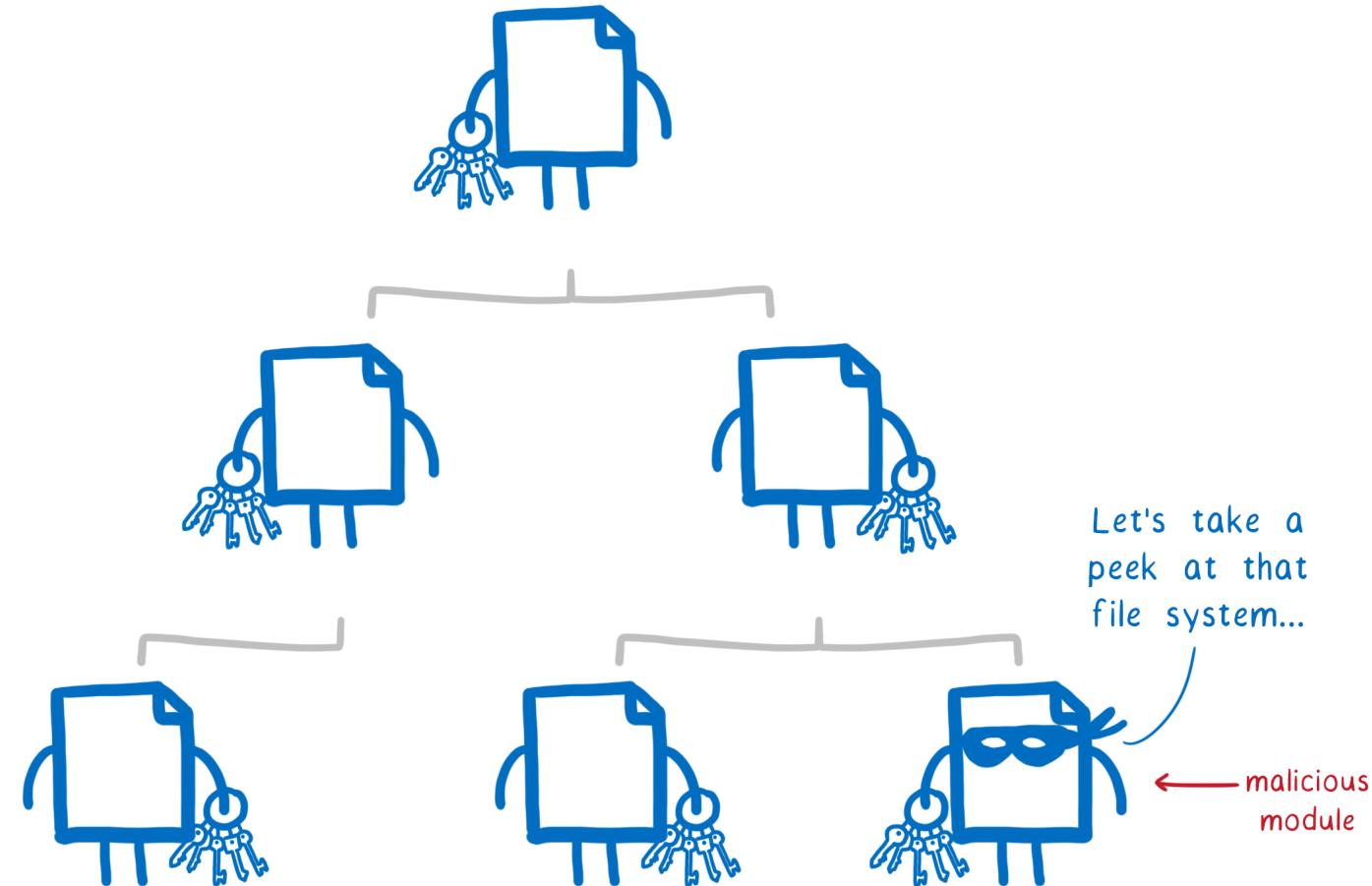


# Average codebase composition





# Malicious Assembly





# Malicious Package

The screenshot shows a web browser window with the title "Hackers target .NET developers with malicious NuGet packages". The article is by Sergiu Gatlan, published on March 20, 2023, at 03:22 PM, with 0 comments. The text discusses threat actors targeting .NET developers with cryptocurrency stealers delivered through the NuGet repository and impersonating multiple legitimate packages via typosquatting. It mentions three packages downloaded over 150,000 times and quotes JFrog security researchers Natan Nehorai and Brian Moussalli. The article also notes the use of typosquatting in package names.

**Hackers target .NET developers with malicious NuGet packages**

By [Sergiu Gatlan](#) March 20, 2023 03:22 PM 0

Threat actors are targeting and infecting .NET developers with cryptocurrency stealers delivered through the NuGet repository and impersonating multiple legitimate packages via typosquatting.

Three of them have been downloaded over 150,000 times within a month, according to JFrog security researchers Natan Nehorai and Brian Moussalli, who spotted this ongoing campaign.

While the massive number of downloads could point to a large number of .NET developers who had their systems compromised, it could also be explained by the attackers' efforts to legitimize their malicious NuGet packages.

"The top three packages were downloaded an incredible amount of times – this could be an indicator that the attack was highly successful, infecting a large amount of machines," the [JFrog security researchers said](#).

"However, this is not a fully reliable indicator of the attack's success since the attackers could have automatically inflated the download count (with bots) to make the packages seem more legitimate."

The threat actors also used typosquatting when creating their NuGet repository profiles to impersonate



# Malicious Package

The screenshot shows a web browser window with the following details:

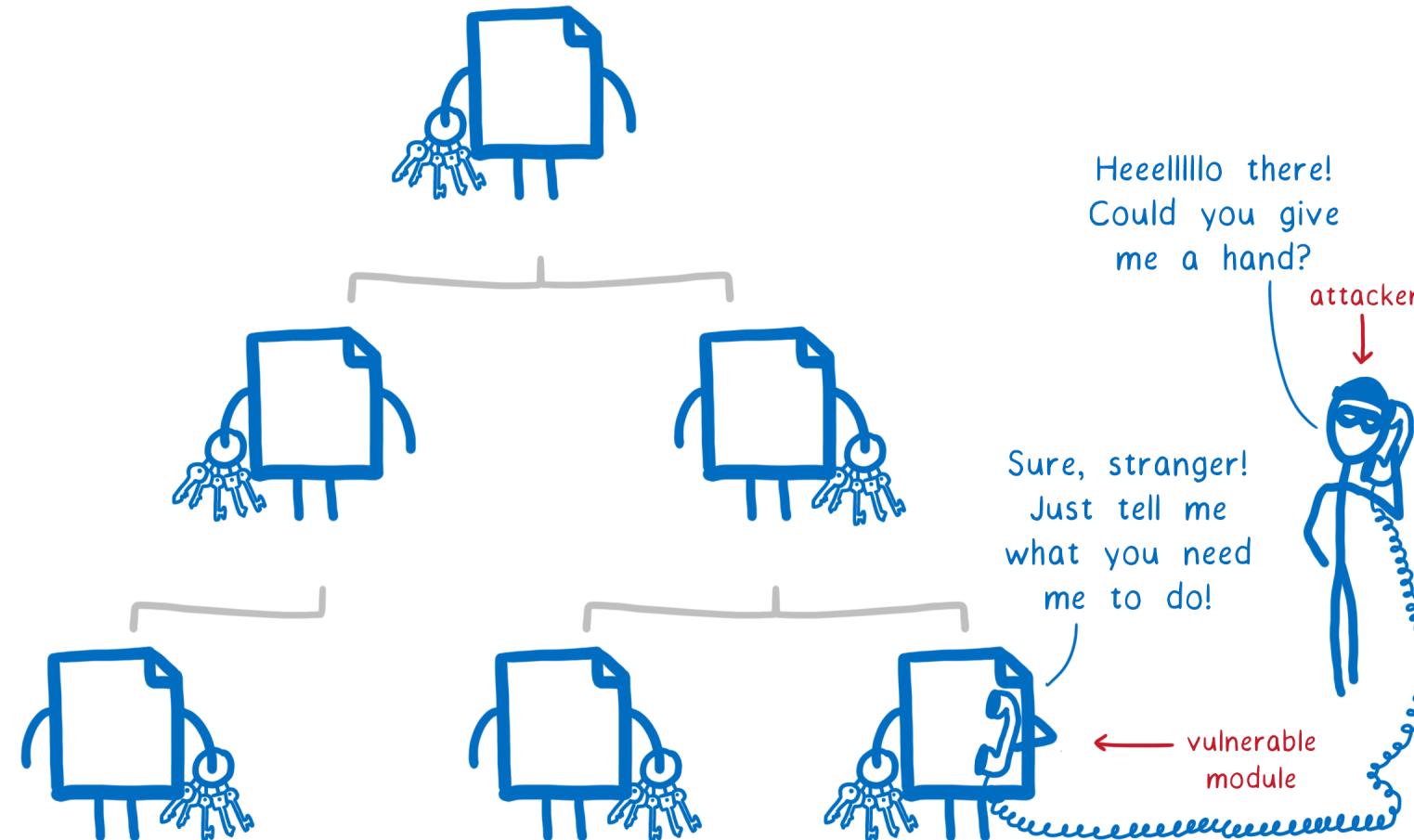
- Title Bar:** IAmReboot: Malicious NuGet pa X
- Address Bar:** https://www.reversinglabs.com/blog/iamreboot-malicious-nuget-packages
- Page Content:**
  - Header:** REVERSINGLABS
  - Section:** Threat Research | October 31, 2023
  - Main Title:** **IAmReboot: Malicious NuGet packages exploit loophole in MSBuild integrations**
  - Text:** ReversingLabs has highlighted threats in npm, PyPI and RubyGEMS in recent years. This finding shows NuGet is equally exposed to malicious activities by threat actors.
  - Bottom Right:** A small purple circular icon with a white upward-pointing arrow.



@nielstanis@infosec.exchange



# Vulnerable Assembly





# Vulnerabilities in Libraries

The screenshot shows a GitHub issue page for Microsoft Security Advisory CVE-2023-36558. The title of the issue is "Microsoft Security Advisory CVE-2023-36558: .NET Security Feature Bypass Vulnerability". The issue was opened by rbhanda on Nov 14 and has 0 comments. A comment from rbhanda is displayed, reiterating the title of the vulnerability. The issue is labeled "Security". The right sidebar shows that no one is assigned to the issue, it has a security label, and no projects or milestones are set. It also indicates that there are no branches or pull requests.

Microsoft Security Advisory CVE-2023-36558: .NET Security Feature Bypass Vulnerability #288

rbhanda commented on Nov 14 · edited

**Microsoft Security Advisory CVE-2023-36558: .NET Security Feature Bypass Vulnerability**

**Executive summary**

Microsoft is releasing this security advisory to provide information about a vulnerability in ASP.NET Core 6.0, ASP.NET Core 7.0 and, ASP.NET Core 8.0 RC2. This advisory also provides guidance on what developers can do to update their applications to address this vulnerability.

A security feature bypass vulnerability exists in ASP.NET where an unauthenticated user is able to bypass validation on Blazor server forms which could trigger unintended actions.

**Discussion**

Discussion for this issue can be found at [dotnet/runtime#94726](#)

Assignees  
No one assigned

Labels  
Security

Projects  
None yet

Milestone  
No milestone

Development  
No branches or pull requests

Notifications  
Customize



@nielstanis@infosec.exchange



# DotNet CLI

```
nelson@ghost-m2 ~/research/consoleapp $ dotnet list package
Project 'consoleapp' has the following package references
[net8.0]:
Top-level Package      Requested    Resolved
> docgenerator          1.0.0        1.0.0

nelson@ghost-m2 ~/research/consoleapp $ dotnet list package --vulnerable

The following sources were used:
https://f.feedz.io/fennec/docgenerator/nuget/index.json
https://api.nuget.org/v3/index.json

The given project `consoleapp` has no vulnerable packages given the current sources.
nelson@ghost-m2 ~/research/consoleapp $
```





# DotNet CLI

```
nelson@ghost-m2 ~/research/consoleapp $ dotnet list package --include-transitive
Project 'consoleapp' has the following package references
[net8.0]:
Top-level Package      Requested   Resolved
> docgenerator        1.0.0       1.0.0

Transitive Package                                     Resolved
> iText7                                         7.2.2
> iText7.common                                     7.2.2
> Microsoft.CSharp                                4.0.1
> Microsoft.DotNet.PlatformAbstractions          1.1.0
> Microsoft.Extensions.DependencyInjection           5.0.0
> Microsoft.Extensions.DependencyInjection.Abstractions 5.0.0
> Microsoft.Extensions.DependencyModel            1.1.0
> Microsoft.Extensions.Logging                     5.0.0
> Microsoft.Extensions.Logging.Abstractions         5.0.0
> Microsoft.Extensions.Options                   5.0.0
> Microsoft.Extensions.Primitives                5.0.0
```





# DotNet CLI

```
nelson@ghost-m2:~/research/consoleapp$ dotnet list package --vulnerable --include-transitive
nelson@ghost-m2 ~/research/consoleapp $ dotnet list package --vulnerable --include-transitive

The following sources were used:
https://f.feedz.io/fennec/docgenerator/nuget/index.json
https://api.nuget.org/v3/index.json

Project `consoleapp` has the following vulnerable packages
[net8.0]:
Transitive Package      Resolved    Severity   Advisory URL
> Newtonsoft.Json        9.0.1       High       https://github.com/advisories/GHSA-5crp-9r3c-p9vr

nelson@ghost-m2 ~/research/consoleapp $
```



@nielstanis@infosec.exchange



# Do you know what's inside?

A screenshot of a web browser window showing a blog post from ReversingLabs. The browser has a dark theme with a red tab bar. The main content area shows the ReversingLabs logo (red square with 'RL') and the title 'ReversingLabs Blog'. Below the title is a sub-header 'Threat Research | July 7, 2021'. The main heading of the post is 'Third-party code comes with some baggage'. A subtitle below it reads 'Recognizing risks introduced by statically linked third-party libraries'. At the bottom, there is a profile picture of a man, a 'BLOG AUTHOR' label, and the name 'Karlo Zanki, Reverse Engineer at ReversingLabs. [READ MORE...](#)'.

Third-party code comes with some baggage

Threat Research | July 7, 2021

Third-party code comes with some baggage

Recognizing risks introduced by statically linked third-party libraries

BLOG AUTHOR  
Karlo Zanki, Reverse Engineer at ReversingLabs. [READ MORE...](#)



@nielstanis@infosec.exchange



# Nutrition Label for Software?





# OpenSSF Scorecards

The screenshot shows a web browser window with the title bar "OpenSSF Scorecard". The address bar displays the URL "https://securityscorecards.dev". The page content features a search bar with the placeholder text "Search openSSF Scorecard", a GitHub star icon with the number "3867", and a large main heading: "Build better security habits, one test at a time". Below this, a subtitle reads "Quickly assess open source projects for risky practices". At the bottom, there are two orange buttons: "Run the checks" and "Learn more".

openssf scorecard

Star 3867

# Build better security habits, one test at a time

Quickly assess open source projects for risky practices

Run the checks Learn more



@nielstanis@infosec.exchange



# OpenSSF Security Scorecards

The screenshot shows a web browser window titled "OpenSSF Scorecard" with the URL <https://securityscorecards.dev/#what-is-openssf-scorecard>. The main content is titled "What is OpenSSF Scorecard?". On the left, there's a sidebar with sections like "Run the checks" (with links to GitHub Action and CLI), "Learn more" (with links to The problem, What is OpenSSF Scorecard?, How it works, The checks, Use cases, About the project name, Part of the OSS community, and Get involved), and two small icons at the bottom.

**What is OpenSSF Scorecard?**

**Run the checks**

Using the GitHub Action  
Using the CLI

**Learn more**

The problem  
[What is OpenSSF Scorecard?](#)  
How it works  
The checks  
Use cases  
About the project name  
Part of the OSS community  
Get involved

Scorecard assesses open source projects for security risks through a series of automated checks

It was created by OSS developers to help improve the health of critical projects that the community depends on.

You can use it to proactively assess and make informed decisions about accepting security risks within your codebase. You can also use the tool to evaluate other projects and dependencies, and work with maintainers to improve codebases you might want to integrate.

Scorecard helps you enforce best practices that can guard against:



 @nielstanis@infosec.exchange



# OpenSSF Security Scorecards

The screenshot shows a web browser window titled "OpenSSF Scorecard" displaying the URL <https://securityscorecards.dev/#how-it-works>. The page content is as follows:

## How it works

### Run the checks

- Using the GitHub Action
- Using the CLI

### Learn more

- The problem
- What is OpenSSF Scorecard?
- How it works** (This item is highlighted in orange)
- The checks
- Use cases
- About the project name
- Part of the OSS community
- Get involved

Scorecard checks for vulnerabilities affecting different parts of the software supply chain including **source code, build, dependencies, testing, and project maintenance**.

Each automated check returns a **score out of 10** and a **risk level**. The risk level **adds a weighting** to the score, and this weighting is compiled into a single, **aggregate score**. This score helps give a sense of the overall security posture of a project.

Alongside the scores, the tool provides remediation prompts to help you **fix problems** and strengthen your development practices.

Risk Level	Score
CRITICAL RISK	10
HIGH RISK	7.5
MEDIUM RISK	5





# OpenSSF Security Scorecards

The screenshot shows a web browser window titled "OpenSSF Scorecard" at the URL <https://securityscorecards.dev/#the-checks>. The page content includes a sidebar with links for "Run the checks" (GitHub Action, CLI) and "Learn more" (The problem, What is OpenSSF Scorecard?, How it works, The checks, Use cases, About the project name, Part of the OSS community, Get involved). To the right of the sidebar is a large graphic consisting of five circles arranged in a pentagonal pattern, all enclosed within a larger red circle. The circles are labeled: "BUILD RISK ASSESSMENT", "CODE VULNERABILITIES", "MAINTENANCE", "CONTINUOUS TESTING", and "SOURCE RISK ASSESSMENT". In the center of the graphic, the words "HOLISTIC SECURITY PRACTICES" are written in orange capital letters.





# Code Vulnerabilities (High)

- Does the project have unfixed vulnerabilities?  
Uses the OSV service.

The screenshot shows a web browser window with the title "NuGet - OSV". The URL in the address bar is <https://osv.dev/list?ecosystem=NuGet>. The page displays a summary of vulnerabilities across various ecosystems:

Ecosystem	Count
Maven	4334
npm	12878
NuGet	545
OSS-Fuzz	3127
Packagist	2392
Pub	6
PyPI	11252
Rocky Linux	1030
RubyGems	746
SwiftURL	29

The main content area shows a table of vulnerabilities for the NuGet ecosystem:

ID	Packages	Summary	Affected versions	Published	Fix	
<a href="#">GHSA-hwcc-4cv8-cf3h</a>	NuGet/Snowflake.Data	Snowflake Connector .NET does not properly check the Certificate Revocation List (CRL)	2.0.25 2.1.1 2.1.3	2.1.0 2.1.2 2.1.4	yesterday	<a href="#">Fix available</a>
<a href="#">GHSA-6xmx-85x3-4cv2</a>	NuGet/Umbraco.CMS	Stored XSS via SVG File Upload	10.0.0 10.0.0-rc2	10.0.0-rc1 10.0.0-rc3	last week	<a href="#">Fix available</a>



@nielstanis@infosec.exchange

# Maintenance Dependency-Update-Tool (**High**)



- This check tries to determine if the project uses a dependency update tool, use of: Dependabot, Renovate bot
- Out-of-date dependencies make a project vulnerable to known flaws and prone to attacks.



# Maintenance Security Policy (Medium)



- Does project have published security policy?
- E.g. a file named **SECURITY.md** (case-insensitive) in a few well-known directories.
- A security policy can give users information about what constitutes a vulnerability and how to report one securely so that information about a bug is not publicly visible.

# Maintenance License (**Low**)



- Does project have license published?
- A license can give users information about how the source code may or may not be used.
- The lack of a license will impede any kind of security review or audit and creates a legal risk for potential users.



# Maintenance CII Best Practices (**Low**)



- OpenSSF Best Practices Badge Program
- Way for Open Source Software projects to show that they follow best practices.
- Projects can voluntarily self-certify, at no cost, by using this web application to explain how they follow each best practice.



openssf best practices **passing**



@nielstanis@infosec.exchange

# Continuous testing

## CI Tests (**Low**)



- This check tries to determine if the project runs tests before pull requests are merged.
- The check works by looking for a set of CI-system names in GitHub CheckRuns and Statuses among the recent commits (~30).



# Continuous testing

## Fuzzing (Medium)



- This check tries to determine if the project uses fuzzing by checking:
  - Added to [OSS-Fuzz](#) project.
  - If [ClusterFuzzLite](#) is deployed in the repository;
  - If there are user-defined language-specified fuzzing functions in the repository.
- Does it make sense to do fuzzing on .NET projects?

# Continuous testing

## Static Code Analysis (Medium)



- This check tries to determine if the project uses Static Application Security Testing (SAST), also known as static code analysis. It is currently limited to repositories hosted on GitHub.
  - CodeQL
  - SonarCloud
- Definitely room for improvement!



# Source Risk Assessment

## Binary Artifacts (**High**)



- This check determines whether the project has generated executable (binary) artifacts in the source repository.
- Binary artifacts cannot be reviewed, allowing possible obsolete or maliciously subverted executables.
- There is need for reproducible builds!



# Source Risk Assessment Branch Protection (**High**)



- This check determines whether a project's default and release branches are protected with GitHub's branch protection or repository rules settings.
  - Requiring code review
  - Prevent force push, in case of public branch all is lost!



# Source Risk Assessment

## Dangerous Workflow (**Critical**)



- This check determines whether the project's GitHub Action workflows has dangerous code patterns.
  - Untrusted Code Checkout with certain triggers
  - Script Injection with Untrusted Context Variables
- <https://securitylab.github.com/research/github-actions-preventing-pwn-requests/>

# Source Risk Assessment

## Code Review (**Low**)



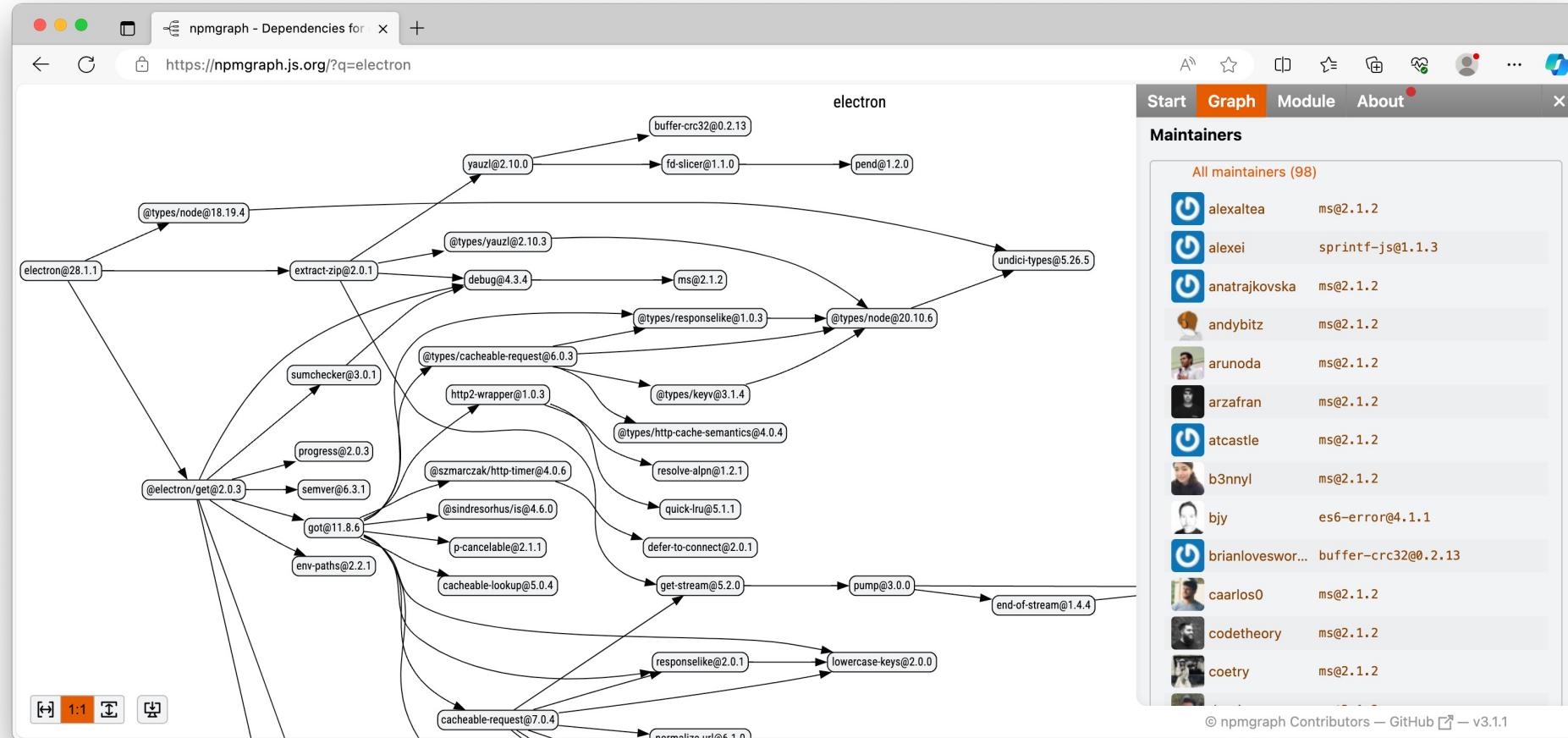
- This check determines whether the project requires human code review before pull requests (merge requests) are merged.
- The check determines whether the most recent changes (over the last ~30 commits) have an approval on GitHub or if the merger is different from the committer (implicit review)

# Source Risk Assessment Contributors (Low)



- This check tries to determine if the project has recent contributors from multiple organizations (e.g., companies).
- Relying on single contributor is a risk
- But is a large list of contributors good?

# Source Risk Assessment Contributors (Low)



@nielstanis@infosec.exchange

# Build Risk Assesement Pinned Dependencies (**High**)



- This check tries to determine if the project pins dependencies used during its build and release process.
- **RestorePackagesWithLockFile** in MSBuild results in packages.lock.json file containing versioned dependency tree with hashes

# Build Risk Assessment Token Permission (High)



- This check determines whether the project's automated workflows tokens follow the principle of least privilege.
- This is important because attackers may use a compromised token with write access to, for example, push malicious code into the project.



# Build Risk Assesement Packaging (Medium)



- This check tries to determine if the project is published as a package.
- Packages give users of a project an easy way to download, install, update, and uninstall the software by a package manager.



# Build Risk Assessment Signed Releases (High)



- This check tries to determine if the project cryptographically signs release artifacts.
  - Signed release packages
  - Signed build provenance



# Demo OpenSSF Scorecard

## Fennec CLI



Running checks



@nielstanis@infosec.exchange



# OpenSSF Annual Report 2023

OpenSSF Scorecard project  
has **3,776 stars** on GitHub,  
and runs a **weekly automated  
assessment scan** against  
software security criteria  
of over **1M OSS projects**



@nielstanis@infosec.exchange



# What can we improve?



 @nielstanis@infosec.exchange

# Fuzzing .NET



- Fuzzing, or fuzz testing, is defined as an automated software testing method that uses a wide range of *invalid* and unexpected data as input to find flaws in the software undergoing the test.
- Used a lot for finding C/C++ memory issues
- Can it be of any value with managed languages like .NET?



# Fuzzing .NET & SharpFuzz

New &  
Improved!



The screenshot shows a web browser window with the following details:

- Title Bar:** Five years of fuzzing .NET with Shar X
- Address Bar:** https://mijailovic.net/2023/07/23/sharpfuzz-anniversary/
- Page Content:**
  - Header:** Nemanja Mijailovic's Blog
  - Section Title:** Five years of fuzzing .NET with SharpFuzz
  - Date:** Jul 23, 2023
  - Text:** It's been almost five years since I created [SharpFuzz](#), the only .NET coverage-guided fuzzer. I already have a blog post on how it works, what it can do for you, and what bugs it found, so check it out if this is the first time you hear about SharpFuzz:  
[SharpFuzz: Bringing the power of afl-fuzz to .NET platform](#)
  - Text:** A lot of interesting things have happened since then. SharpFuzz now works with libFuzzer, Windows, and .NET Framework. And it can finally fuzz the .NET Core base-class library! The whole fuzzing process has been dramatically simplified, too.
  - Text:** Not many people are aware of all these developments, so I decided to write this anniversary blog post and showcase everything SharpFuzz is currently capable of.



@nielstanis@infosec.exchange

# Fuzzing .NET & SharpFuzz

New &  
Improved!



The screenshot shows a web browser window with the title bar "Five years of fuzzing .NET with Shar". The URL in the address bar is <https://mijailovic.net/2023/07/23/sharpfuzz-anniversary/>. The main content area has a heading "Trophies". Below it, a paragraph discusses the growth of bugs found by SharpFuzz, mentioning over 80 entries. It highlights that some bugs in the .NET Core standard library would have been impossible to discover using other methods. A bulleted list follows:

- [BigInteger.TryParse out-of-bounds access](#)
- [Double.Parse throws AccessViolationException on .NET Core 3.0](#)
- [G17 format specifier doesn't always round-trip double values](#)

As you can see, SharpFuzz is capable of finding not only crashes, but also correctness bugs—the more creative you are in writing your fuzzing functions, the higher your chances are for finding an interesting bug.

SharpFuzz can also find serious security vulnerabilities. I now have two CVEs in my trophy collection:

- [CVE-2019-0980: .NET Framework and .NET Core Denial of Service Vulnerability](#)
- [CVE-2019-0981: .NET Framework and .NET Core Denial of Service Vulnerability](#)

If you were ever wondering if fuzzing managed languages makes sense, I think you've got your answer right here.



@nielstanis@infosec.exchange



# Fuzzing .NET - Jil JSON Serializer

```
public static void Main(string[] args)
{
    SharpFuzz.Fuzzer.OutOfProcess.Run(stream => {
        try
        {
            using (var reader = new System.IO.StreamReader(stream))
                JSON.DeserializeDynamic(reader);
        }
        catch (DeserializationException) { }
    });
}
```





New &  
Improved!

# Fuzzomatic: Using AI to Fuzz Rust

The screenshot shows a web browser window with the title "Introducing Fuzzomatic: Using / X" and the URL "https://research.kudelskisecurity.com/2023/12/07/introducing-fuzzomatic-using-ai-to-automatically-fuzz-rust-projects-from-scratch/". The page content is as follows:

## How does it work?

Fuzzomatic relies on libFuzzer and cargo-fuzz as a backend. It also uses a variety of approaches that combine AI and deterministic techniques to achieve its goal.

We used the OpenAI API to generate and fix fuzz targets in our approaches. We mostly used the gpt-3.5-turbo and gpt-3.5-turbo-16k models. The latter is used as a fallback when our prompts are longer than what the former supports.

### Fuzz targets and coverage-guided fuzzing

The output of the first step is a source code file: a fuzz target. A libFuzzer fuzz target in Rust looks like this:

```
1  #![no_main]
2  extern crate libfuzzer_sys;
3  use mylib_under_test::MyModule;
4  use libfuzzer_sys::fuzz_target;
5  fuzz_target!(data: &[u8]) {
6      // fuzzed code goes here
7      if let Ok(input) = std::str::from_utf8(data) {
8          MyModule::target_function(input);
9      }
10 }
11 };
```

This fuzz target needs to be compiled into an executable. As you can see, this program depends on libFuzzer and also depends on the library under test, here "mylib\_under\_test". The "fuzz\_target!" macro makes it easy for us to just write what needs to be called, provided that we receive a byte slice, the "data" variable in the above example. Here we convert these bytes to a UTF-8 string and call our target function and pass that string as an argument. LibFuzzer takes care of calling our fuzz target repeatedly with random bytes. It measures the code coverage to assess whether the random input helps cover more code. We say it's coverage-guided fuzzing.

Comment Reblog Subscribe ...



@nielstanis@infosec.exchange

# Static Code Analysis (SAST)



```
public byte[] CreateHash(string password)
{
    var b = Encoding.UTF8.GetBytes(password);
    return SHA1.HashData(b);
}
```





New &  
Improved!

# Static Code Analysis (SAST)

```
public class CustomerController : Controller
{
    public IActionResult GenerateCustomerReport(string customerID)
    {
        var data = Reporting.GenerateCustomerReportOverview(customerID)
        return View(data);
    }
    public static class Reporting
    {
        public static byte[] GenerateCustomerReportOverview(string ID)
        {
            return System.IO.File.ReadAllBytes("./data/{ID}.pdf");
        }
    }
}
```



# .NET Reproducibility



- Reproducible builds are a set of software development practices that create an independently-verifiable path from source to binary code.
- .NET Roslyn Deterministic Inputs
- How reproducible is a simple console app?



# Application Inspector

New & Improved!



The screenshot shows the Microsoft Application Inspector interface running in a Microsoft Edge browser window. The title bar reads "Microsoft Application Ir" and the address bar shows "file:///C:/Demo/Appinspector/publish/output.html#". The main content area has a header "Application Features" with a sub-instruction about viewing application characteristics by feature group. Below this is a "Feature Groups" section containing ten categories with their respective icons: "Select Features", "General Features", "Development", "Active Content", "Data Storage", "Sensitive Data", "Cloud Services", "OS Integration", "OS System Changes", and "Other". To the right of this is an "Associated Rules" section with a table:

Name (click to view source)
Authentication: Microsoft (Identity)
Authentication: General
Authentication: (Oauth)



@nielstanis@infosec.exchange



New &  
Improved!

# Application Inspector

## Select Features

Feature	Confidence	Details
Authentication		<a href="#">View</a>
Authorization		<a href="#">View</a>
Cryptography		<a href="#">View</a>
Object Deserialization		N/A
AV Media Parsing		N/A
Dynamic Command Execution		N/A



@nielstanis@infosec.exchange

# Community Review



The screenshot shows a web browser window displaying the "Cargo Vet" documentation at <https://mozilla.github.io/cargo-vet/>. The page has a dark theme. On the left, there is a navigation sidebar with sections like "1. Introduction", "2. Tutorial", and "3. Reference". The main content area is titled "Cargo Vet" and contains text about the tool's purpose, how it works, and its key features, such as sharing findings and performing relative audits.

**Cargo Vet**

The `cargo vet` subcommand is a tool to help projects ensure that third-party Rust dependencies have been audited by a trusted entity. It strives to be lightweight and easy to integrate.

When run, `cargo vet` matches all of a project's third-party dependencies against a set of audits performed by the project authors or entities they trust. If there are any gaps, the tool provides mechanical assistance in performing and documenting the audit.

The primary reason that people do not ordinarily audit open-source dependencies is that it is too much work. There are a few key ways that `cargo vet` aims to reduce developer effort to a manageable level:

- **Sharing:** Public crates are often used by many projects. These projects can share their findings with each other to avoid duplicating work.
- **Relative Audits:** Different versions of the same crate are often quite similar to each other. Developers can inspect the difference between two versions, and record that if the first version was vetted, the second can be considered vetted as well.
- **Deferred Audits:** It is not always practical to achieve full coverage. Dependencies can be added to a list of exceptions which can be ratcheted down over time. This makes it trivial to introduce `cargo vet` to a new project and guard against future vulnerabilities while vetting the



@nielstanis@infosec.exchange



# Conclusion

- Scorecard helps out to security review a NuGet Package
- Better understand what's inside, how it's build/maintained and what are the risks!
- Scorecard should not be a goal on its own!
- NuGet Package Scoring (NET Score)
- Room for .NET specific improvements with Fennec CLI & contributions to OpenSSF Scorecard project





# Questions?





# Thanks!

- <https://github.com/nielstanis/bitbash2024/>
- ntanis at Veracode.com
- @nielstanis@infosec.exchange
- <https://www.fennec.dev> & <https://blog.fennec.dev>
- Bedankt! Thank you!

