



Reviewing NuGet Packages security easily using OpenSSF Scorecard

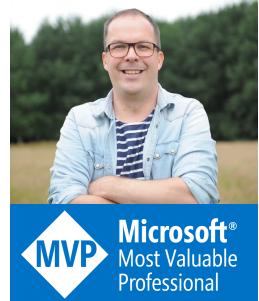
Niels Tanis
Sr. Principal Security Researcher



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



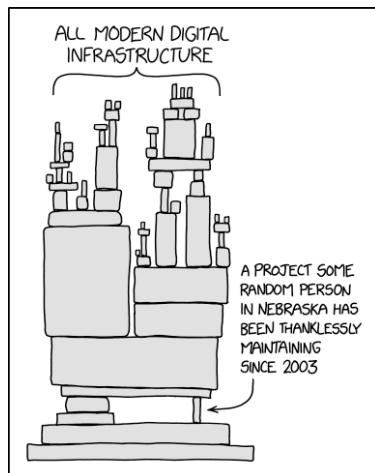
MVP Microsoft®
Most Valuable
Professional

ElevateDev'24

 @nielstanis@infosec.exchange

Modern Application Architecture XKCD 2347

ElevateDev'24



 @nielstanis@infosec.exchange

<https://xkcd.com/2347/>

Agenda

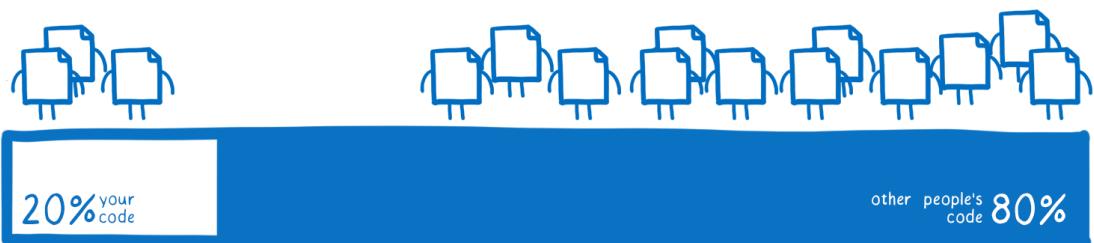
- Risks in 3rd party NuGet Packages
- OpenSFF Scorecard
- New & Improved
- Conclusion - Q&A



 @nielstanis@infosec.exchange

ElevateDev'24

Average codebase composition



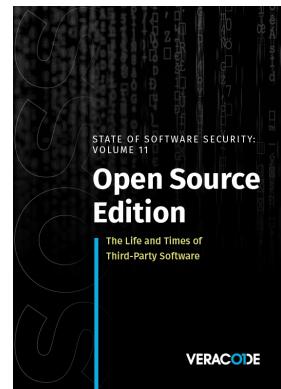
ElevateDev'24

 @nielstanis@infosec.exchange

<https://hacks.mozilla.org/2019/11/announcing-the-bytecode-alliance/>

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."



ElevateDev'24

@nielstanis@infosec.exchange

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.

ElevateDev'24

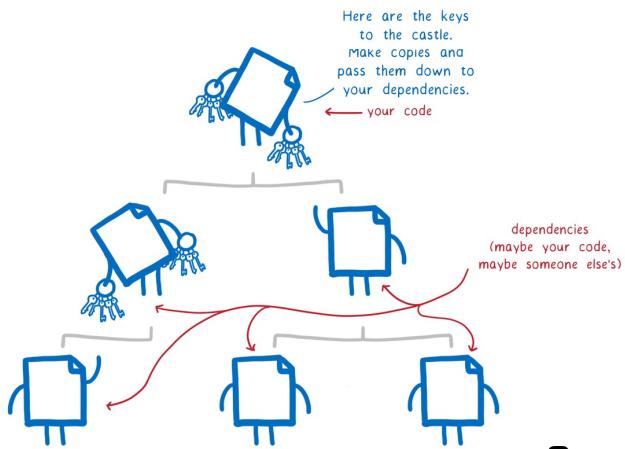
 @nielstanis@infosec.exchange

<https://www.veracode.com/blog/research/state-log4j-vulnerabilities-how-much-did-log4shell-change>

Average codebase composition

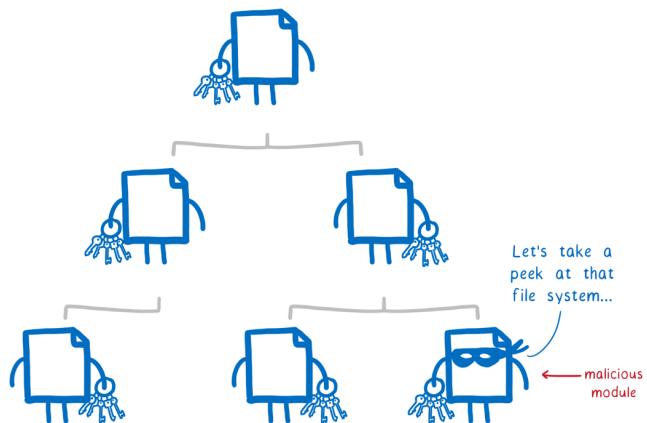
ElevateDev'24

 @nielstanis@infosec.exchange



<https://hacks.mozilla.org/2019/11/announcing-the-bytecode-alliance/>

Malicious Assembly



ElevateDev'24

 @nielstanis@infosec.exchange

<https://hacks.mozilla.org/2019/11/announcing-the-bytecode-alliance/>

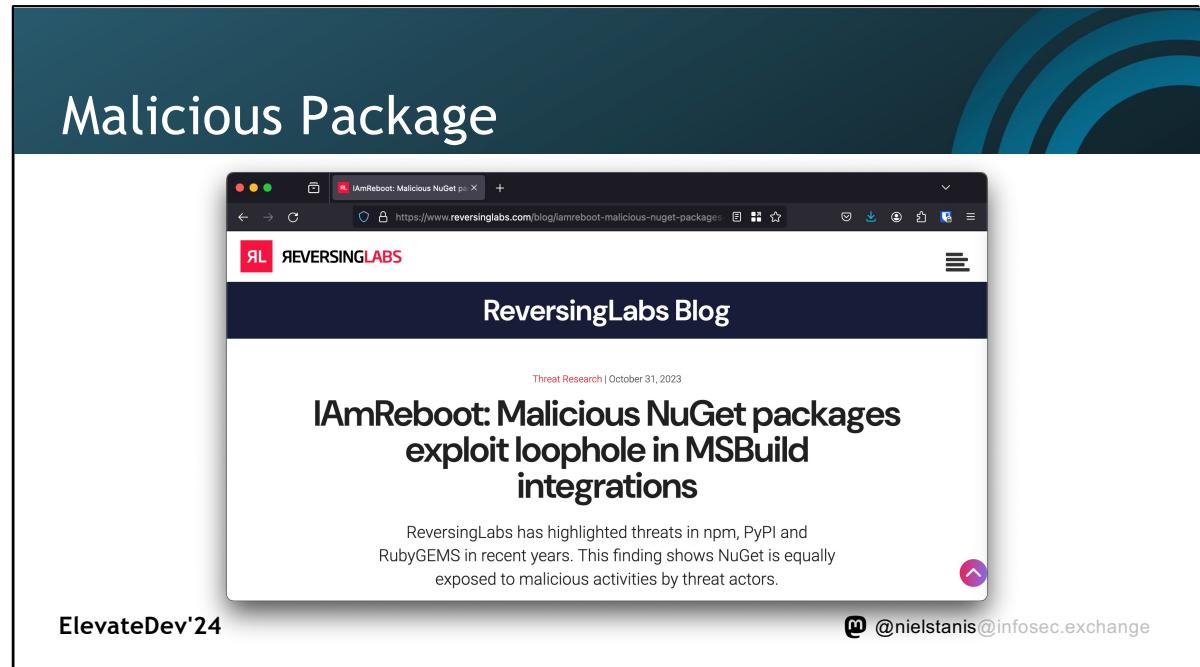
Malicious Package

The screenshot shows a news article titled "Hackers target .NET developers with malicious NuGet packages" published by Sergiu Gatlan on March 20, 2023, at 03:22 PM. The article discusses threat actors targeting .NET developers with cryptocurrency stealers delivered through the NuGet repository and impersonating multiple legitimate packages via typosquatting. It mentions that over 150,000 packages have been downloaded within a month. Researchers Natan Nehorai and Brian Moussalli spotted the ongoing campaign. The article notes that while the massive number of downloads could point to a large number of .NET developers, it could also be explained by attackers' efforts to legitimize their malicious NuGet packages. Quoted researchers say the top three packages were downloaded an incredible amount of times, which could be an indicator of success. The attackers inflated download counts with bots to make the packages seem more legitimate. The threat actors also used typosquatting when creating their NuGet repository profiles to impersonate legitimate ones.

ElevateDev'24

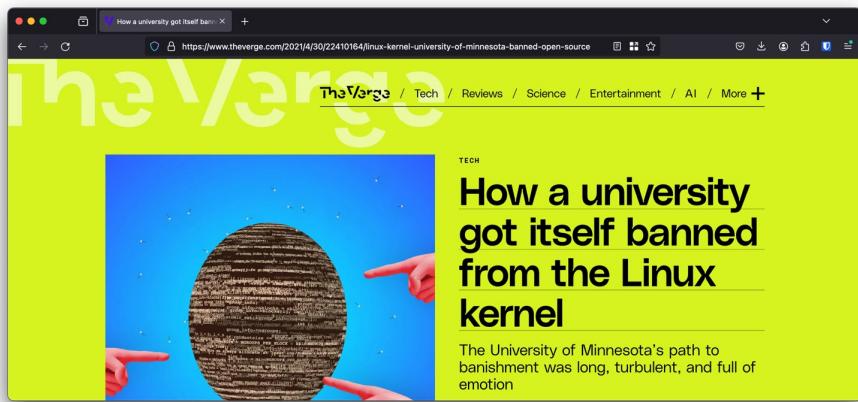
@nielstanis@infosec.exchange

[https://www.bleepingcomputer.com/news/security/hackers-target-net-developers-with-malicious-nuget-packages//](https://www.bleepingcomputer.com/news/security/hackers-target-net-developers-with-malicious-nuget-packages/)



<https://www.reversinglabs.com/blog/iamreboot-malicious-nuget-packages-exploit-msbuild-loophole>

Hypocrite Commits



ElevateDev'24

 @nielstanis@infosec.exchange

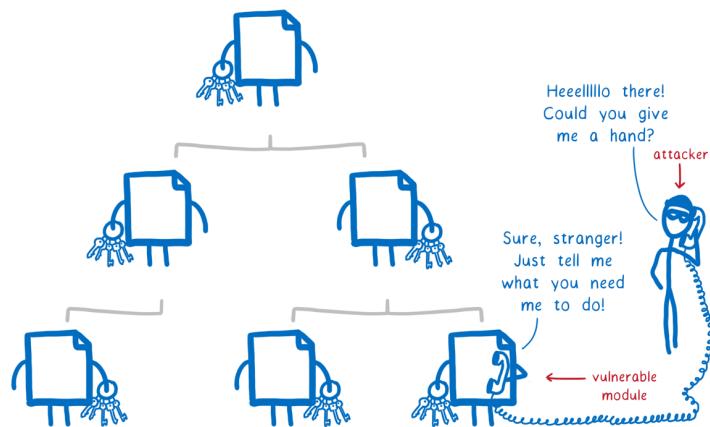
<https://www.theverge.com/2021/4/30/22410164/linux-kernel-university-of-minnesota-banned-open-source>

XZ Backdoor

The screenshot shows a web browser window displaying an Ars Technica article. The title of the article is "Backdoor found in widely used Linux utility targets encrypted SSH connections". The article is categorized under "SUPPLY CHAIN ATTACK". A sub-headline states: "Malicious code planted in xz Utils has been circulating for more than a month." The author is listed as "DAN GOODIN - 3/29/2024, 7:50 PM". The Ars Technica logo is visible at the top left, and there are "SUBSCRIBE", "SIGN IN", and search icons at the top right. The background of the page features a dark blue gradient with abstract blue wave patterns.

<https://arstechnica.com/security/2024/03/backdoor-found-in-widely-used-linux-utility-breaks-encrypted-ssh-connections/>

Vulnerable Assembly

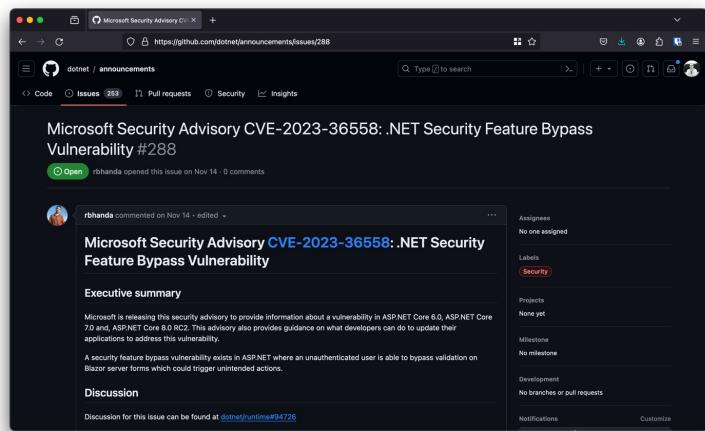


ElevateDev'24

@nielstanis@infosec.exchange

<https://hacks.mozilla.org/2019/11/announcing-the-bytecode-alliance/>

Vulnerabilities in Libraries



ElevateDev'24

@nielstanis@infosec.exchange

<https://github.com/dotnet/announcements/issues/288>

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 $
```

ElevateDev'24

 @nielstanis@infosec.exchange

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
```

ElevateDev'24

 @nielstanis@infosec.exchange

DotNet CLI

```
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 $
```

ElevateDev'24

 @nielstanis@infosec.exchange

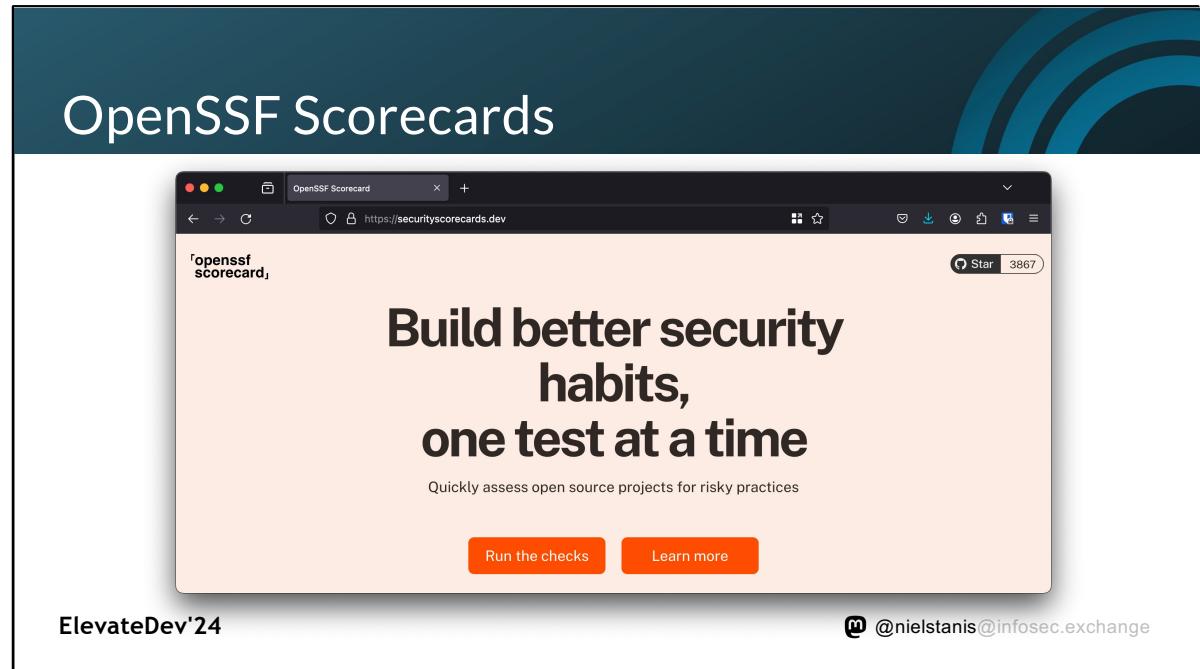
Do you know what's inside?

The screenshot shows a web browser window with a dark blue header banner containing the text "Do you know what's inside?". Below the banner is a white content area. At the top of the content area is the ReversingLabs logo and a navigation menu. The main title of the blog post is "Third-party code comes with some baggage", with a subtitle "Recognizing risks introduced by statically linked third-party libraries". Below the title is a author bio for Karlo Zanki, Reverse Engineer at ReversingLabs. At the bottom left of the content area, there is a "ElevateDev'24" watermark. At the bottom right, there is a Twitter icon and the handle "@nielstanis@infosec.exchange".

<https://www.reversinglabs.com/blog/third-party-code-comes-with-some-baggage>

Nutrition Label for Software?





<https://securityscorecards.dev/>

The screenshot shows a web browser window with the title "OpenSSF Security Scorecards". The main content area displays the "What is OpenSSF Scorecard?" page. On the left, there is a sidebar with sections for "Run the checks" (Using the GitHub Action, Using the 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). The main content area has three columns: "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.", and "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." Below the content are two small icons: a red circle with a white dot and a grid of squares.

ElevateDev'24

@nielstanis@infosec.exchange

<https://securityscorecards.dev/>

The screenshot shows a web browser window titled "OpenSSF Scorecard" with the URL <https://securityscorecards.dev/#how-it-works>. The page has a dark blue header with the text "OpenSSF Security Scorecards". Below the header is a light orange section titled "How it works". On the left side of this section, there are two columns of links: "Run the checks" (Using the GitHub Action, Using the 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 these links, there is explanatory text about how the scorecard checks for vulnerabilities across the software supply chain and how automated checks return a score out of 10 and a risk level. It also mentions that the tool provides remediation prompts. At the bottom of this section, there are three horizontal bars representing risk levels: "CRITICAL RISK" (value 10), "HIGH RISK" (value 7.5), and "MEDIUM RISK" (value 5). The footer of the page includes the text "ElevateDev'24" on the left and "@nielstanis@infosec.exchange" with a profile icon on the right.

<https://securityscorecards.dev/>

OpenSSF Security Scorecards

The screenshot shows a web browser window titled "OpenSSF Scorecard" at the URL <https://securityscorecards.dev/#the-checks>. On the left, there's a sidebar with sections for "Run the checks" (GitHub Action, CLI) and "Learn more" (problem, what it is, how it works, checks, use cases, project name, community, get involved). The main content area features a large diagram. In the center is a red circle containing the text "HOLISTIC SECURITY PRACTICES". Five smaller white circles are arranged around it, each with a black outline: "CODE VULNERABILITIES" (top), "BUILD RISK ASSESSMENT" (left), "MAINTENANCE" (right), "SOURCE RISK ASSESSMENT" (bottom-left), and "CONTINUOUS TESTING" (bottom-right). At the bottom left of the slide, the text "ElevateDev'24" is visible, and at the bottom right, there's a small icon and the email address "@nielstanis@infosec.exchange".

<https://securityscorecards.dev/>

Code Vulnerabilities (High)

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

ID	Packages	Summary	Affected versions	Published	Fix
GHSA-x674-1x45-1eww	NuGet/Microsoft.Identity.Client	MSAL.NET applications targeting Xamarin Android and .NET Android (MAUI) susceptible to local denial of service	4.46.0 4.49.0 4.50.0 4.52.0	4.48.1 4.49.1 4.51.0 —	9 hours ago Fix available
GHSA-5x7m-6727-26ct	NuGet/SixLabors.ImageSharp	SixLabors.ImageSharp vulnerable to data leakage	1.0.0 1.0.0-beta0002 1.0.0-beta0004 1.0.0-beta0006	1.0.0-beta0001 1.0.0-beta0003 1.0.0-beta0005 —	yesterday Fix available
GHSA-q85r-6x2g-45w7	NuGet/SixLabors.ImageSharp	SixLabors.ImageSharp vulnerable to Memory Allocation with Excessive Size Value	1.0.0 1.0.0-beta0002 1.0.0-beta0004 1.0.0-beta0006	1.0.0-beta0001 1.0.0-beta0003 1.0.0-beta0005 —	yesterday Fix available

ElevateDev'24

 @nielstanis@infosec.exchange

<https://osv.dev/list?ecosystem=NuGet>

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

- Does the project use a dependency update tool?
For example Dependabot or Renovate bot?
- Out-of-date dependencies make a project vulnerable to known flaws and prone to attacks.

ElevateDev'24

 @nielstanis@infosec.exchange

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.

ElevateDev'24

 @nielstanis@infosec.exchange

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.

ElevateDev'24

 @nielstanis@infosec.exchange

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

ElevateDev'24

<https://www.bestpractices.dev/en/criteria/0>

Continuous testing CI Tests (**Low**)

- Does the project run 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).

ElevateDev'24

 @nielstanis@infosec.exchange

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?

ElevateDev'24

 @nielstanis@infosec.exchange

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!

ElevateDev'24

 @nielstanis@infosec.exchange

Source Risk Assesement 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!

ElevateDev'24

 @nielstanis@infosec.exchange

Source Risk Assesement 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!

ElevateDev'24

 @nielstanis@infosec.exchange

Source Risk Assesement 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/>

ElevateDev'24

 @nielstanis@infosec.exchange

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)

ElevateDev'24

 @nielstanis@infosec.exchange

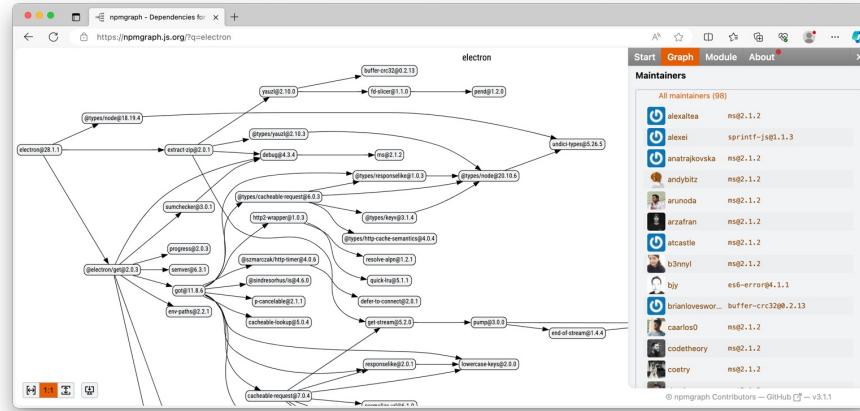
Source Risk Assessment Contributors (Low)

- 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?

ElevateDev'24

 @nielstanis@infosec.exchange

Source Risk Assessment Contributors (Low)



ElevateDev'24

@nielstanis@infosec.exchange

Build Risk Assessment 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
- If Workflow is present what about the Actions used?

ElevateDev'24

 @nielstanis@infosec.exchange

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.

ElevateDev'24

 @nielstanis@infosec.exchange

<https://securitylab.github.com/research/github-actions-preventing-pwn-requests/>

Build Risk Assessment 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.

ElevateDev'24

 @nielstanis@infosec.exchange

Build Risk Assessment Signed Releases (**High**)

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

ElevateDev'24

 @nielstanis@infosec.exchange

Demo OpenSSF Scorecard Fennec CLI

Running checks



ElevateDev'24

@nielstanis@infosec.exchange

<https://www.bestpractices.dev/en/criteria/0>

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**



ElevateDev'24

@nielstanis@infosec.exchange

<https://openssf.org/download-the-2023-openssf-annual-report/>

What can we improve?



ElevateDev'24

 @nielstanis@infosec.exchange

<https://www.bestpractices.dev/en/criteria/0>

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?

ElevateDev'24

 @nielstanis@infosec.exchange

<https://www.bestpractices.dev/en/criteria/0>

Fuzzing .NET & SharpFuzz

New & Improved!

Nemanja Mijailovic's Blog

Five years of fuzzing .NET with SharpFuzz

Jul 23, 2023

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](#)

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.

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.

ElevateDev'24

@nielstanis@infosec.exchange

<https://mijailovic.net/2023/07/23/sharpfuzz-anniversary/>

Fuzzing .NET & SharpFuzz

New & Improved!

Trophies

The list of bugs found by SharpFuzz has been growing steadily and it now contains more than 80 entries. I'm pretty confident that some of the bugs in the .NET Core standard library would have been impossible to discover using any other testing method:

- 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.

ElevateDev'24

@nielstanis@infosec.exchange

<https://mijailovic.net/2023/07/23/sharpfuzz-anniversary/>

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) { }
    });
}
```

ElevateDev'24

 @nielstanis@infosec.exchange

<https://github.com/google/fuzzing/blob/master/docs/structure-aware-fuzzing.md>

Fuzzomatic: Using AI to Fuzz Rust

New & Improved!

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
6  fuzz_target!(data: [u8]) {
7      // Fuzzed code goes here
8      if let Ok(input) = std::str::from_utf8(data) {
9          MyModule::target_function(input);
10     }
11 }
12 }
```

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.

ElevateDev'24

@nielstanis@infosec.exchange

<https://research.kudelskisecurity.com/2023/12/07/introducing-fuzzomatic-using-ai-to-automatically-fuzz-rust-projects-from-scratch/>

Static Code Analysis (SAST)



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

ElevateDev'24

@nielstanis@infosec.exchange

<https://www.bestpractices.dev/en/criteria/0>

Static Code Analysis (SAST)

New &
Improved!

```
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");
    }
}
```

ElevateDev'24

 @nielstanis@infosec.exchange

<https://www.bestpractices.dev/en/criteria/0>

.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?

ElevateDev'24

 @nielstanis@infosec.exchange

ElevateDev'24

@nielstanis@infosec.exchange

<https://github.com/microsoft/ApplicationInspector>

Application Inspector

New &
Improved!

— Select Features	Feature	Confidence	Details
	Authentication		View
	Authorization		View
	Cryptography		View
	Object Deserialization		N/A
	AV Media Parsing		N/A
	Dynamic Command Execution		N/A

ElevateDev'24

@nielstanis@infosec.exchange

<https://github.com/microsoft/ApplicationInspector>

The screenshot shows a web browser displaying the [Cargo Vet](https://mozilla.github.io/cargo-vet/) documentation. The page has a dark theme with a sidebar on the left containing a table of contents. A red starburst badge in the top right corner says "New & Improved!". The main content area is titled "Cargo Vet" and discusses the tool's purpose and features, including sharing, relative audits, and deferred audits.

ElevateDev'24

@nielstanis@infosec.exchange

<https://mozilla.github.io/cargo-vet/>

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



ElevateDev'24

 @nielstanis@infosec.exchange

Questions?



ElevateDev'24

 @nielstanis@infosec.exchange

Links

- <https://github.com/nielstanis/elevatedev24nuget/>
- ntanis at Veracode.com
- @nielstanis@infosec.exchange
- <https://www.fennec.dev> & <https://blog.fennec.dev>

ElevateDev'24

 @nielstanis@infosec.exchange