Duende.

Building a supply chain attack with .NET and NuGet

Maarten Balliauw
Bluesky: @maartenballiauw.be

Duende.

What is a software supply chain attack?

Duende.

What is a software supply chain attack?

- **Attack elements in the software supply network**
  - Legitimate libraries, tools, vendors, …
- **Add a malicious payload**
  - Data theft, ransomware, system control, …
- **Impact downstream from the vendor to the ultimate targets**
- **Often carried out via “sleeper” approach**

Duende.

Recent examples

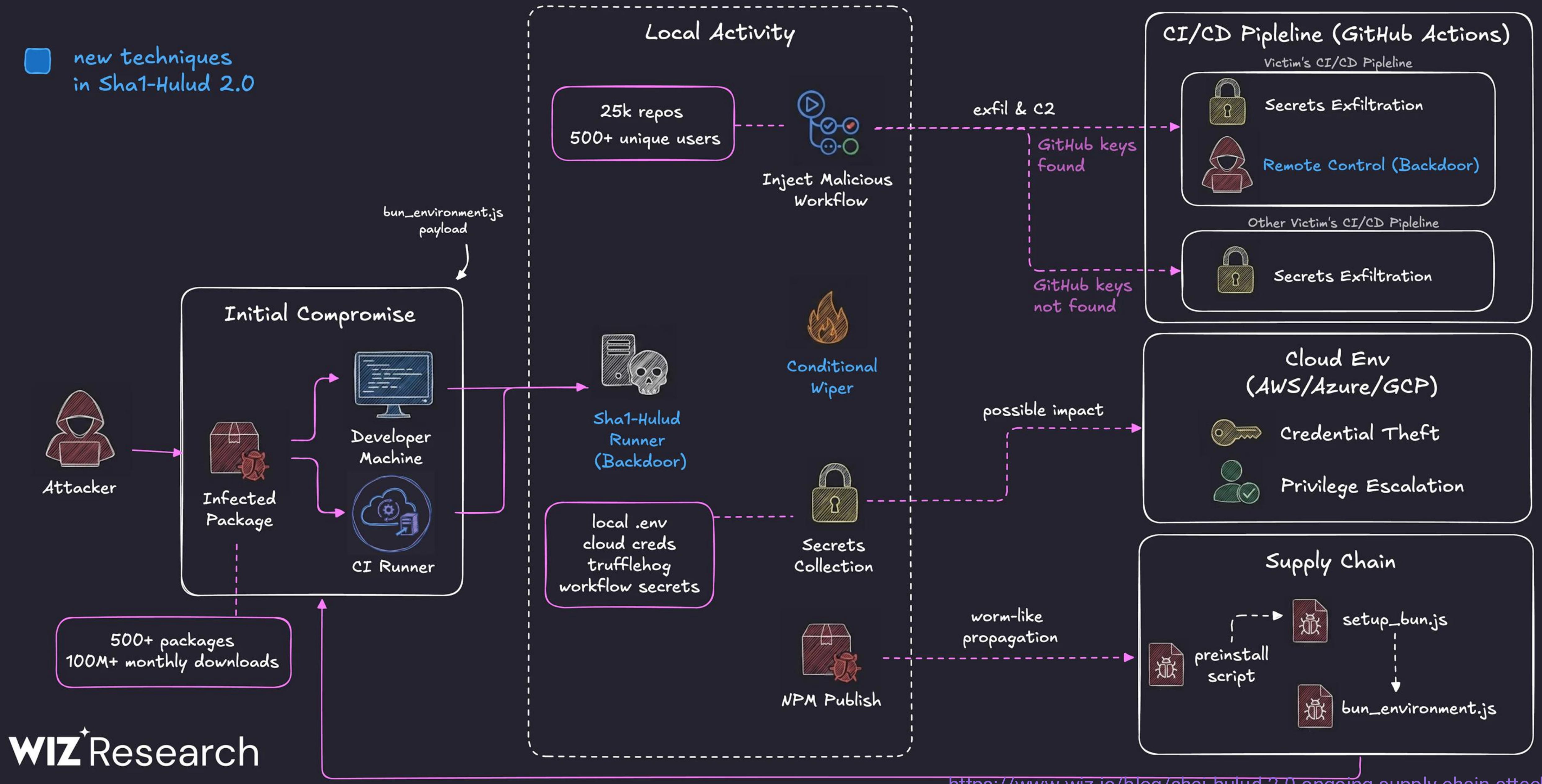
- **SolarWinds Orion**
  - Compromised CI/build infrastructure
  - Smuggled malicious code into the product shipped to customers
  - Access to customer IT systems

Duende.

Recent examples

- **npm “Shai Hulud” attack**
  - Compromised several dependencies of widely-used npm packages
  - In turn compromises packages on developer machine
  - Steal/exfiltrate data (cloud credentials, GitHub credentials, other secrets, …) + manipulate cloud IAM + remote control

SHA1-HULUD 2.0: ONGOING SUPPLY CHAIN ATTACK



WIZ Research

https://www.wiz.io/blog/shai-hulud-2-0-ongoing-supply-chain-attack

Duende.

Observations

- **Infiltrate dependencies + dependency confusion**
- **Use npm's `postinstall` hook to run code**
  - Infect dependent package
  - Run payload
- **Use GitHub as Command and Control infrastructure**
  - Repos to store exfiltrated data
  - GitHub Actions and Discussions to execute further commands

dropper

C2 infrastructure

Duende.

Usual components

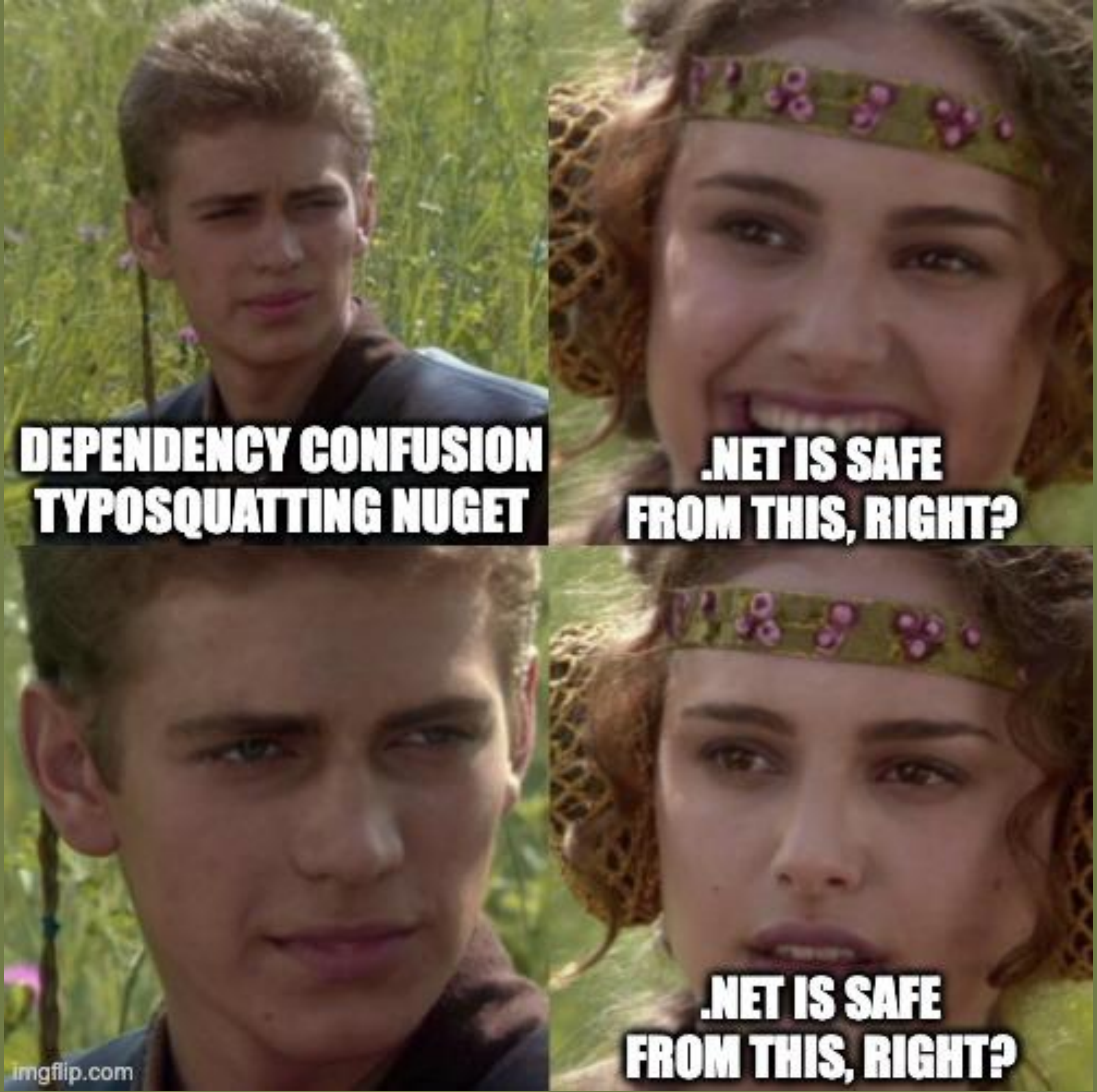
- **Dropper – the initial code executed on the victim's machine**
  - Ideally stealthy, establishes a foothold
- **Payload – action(s) to perform, often received via C2**
  - Collect environment variables, look at files, traverse network, invoke commands, …
- **C2 (Command & Control) infrastructure – receive instructions/payload**
  - Ideally stealthy or expected traffic

Duende.

Infection vectors

- **Gain access to source code, CI/build, … through various means**
  - Social engineering, pull requests, …
  - Compromise maintainer account
- **Dependency Confusion**
  - Publish private package names to public registry, this will often take precedence over internal registry
- **Typosquatting**
  - `Newtonsoft.Jason`, `Microsoft.EntityFrameworkCore`, …

Ukrainian dotted i,
not to be confused with i


DEPENDENCY CONFUSION
TYPOSQUATTING NUGET
.NET IS SAFE
FROM THIS, RIGHT?
.NET IS SAFE
FROM THIS, RIGHT?
imgflip.com

Duende.

Dependency Confusion

Duende.

NuGet package resolution

- **Searches all configured package sources**
- **Non-deterministic when package exists in multiple sources**
- `AcmeCorp.Framework` **on a private package source and on NuGet.org**
    - A good chance the NuGet.org version will be downloaded

Duende.

Use package source mapping

https://learn.microsoft.com/en-us/nuget/consume-packages/package-source-mapping

```xml
<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <packageSources>
        <clear />
        <add key="nuget.org" value="https://api.nuget.org/v3/index.json" />
        <add key="duende-internal" value="https://..../" />
    </packageSources>
    <packageSourceMapping>
        <packageSource key="nuget.org">
            <package pattern="*" />
        </packageSource>
        <packageSource key="duende-internal">
            <package pattern="Duende.*" />
        </packageSource>
    </packageSourceMapping>
</configuration>
```

Duende.

Package signing and verification

- **Packages signed with timestamp + certificate**
- **Different trust options**
  - Whole repo
  - Package author
  - Package owner

https://learn.microsoft.com/en-us/nuget/create-packages/sign-a-package

https://learn.microsoft.com/en-us/nuget/consume-packages/installing-signed-packages

Duende.

Register private package ID prefix

- **Avoid package uploads with your company/project prefix**
- **E.g. `AcmeCorp.*`**

https://learn.microsoft.com/en-us/nuget/nuget-org/id-prefix-reservation

Duende.

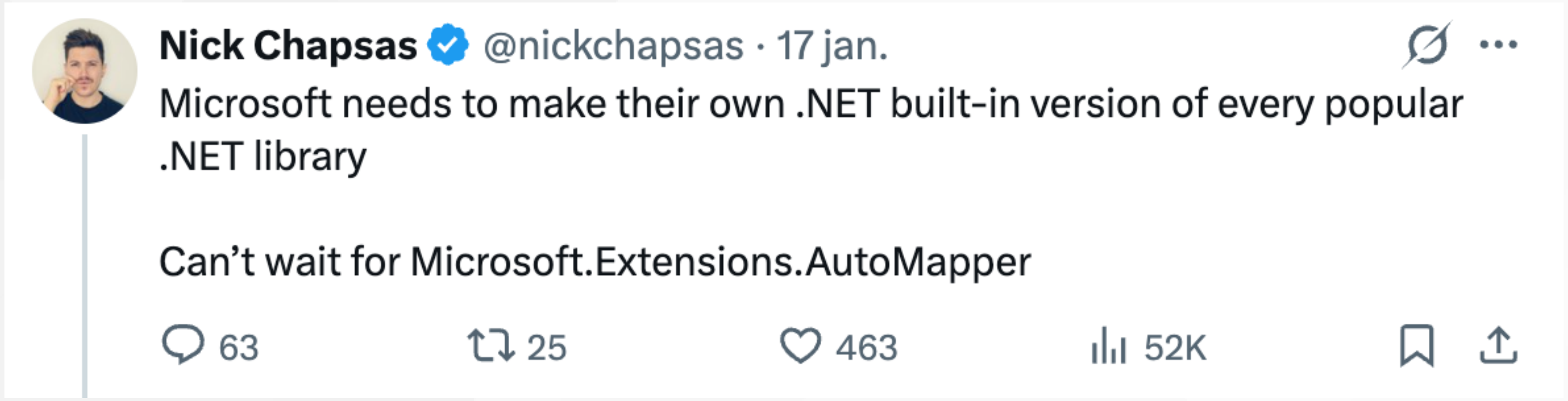
Dependency Confusion mitigations

- **Use package source mapping**
- **Use package signing**
- **Register package ID prefix**
- `RestorePackagesWithLockFile` **+** `RestoreLockedMode` **on CI**

Duende.

Typosquatting

Early 2025…



Nick Chapsas @nickchapsas · 17 jan.

Microsoft needs to make their own .NET built-in version of every popular .NET library

Can’t wait for Microsoft.Extensions.AutoMapper

https://x.com/nickchapsas/status/1880205372470001822

Duende.

Early 2025…

https://gist.github.com/StevenACoffman/a5f6f682d94e38ed804182dc2693ed4b

a a, a, ạ, ą, ä, à, á, □, □, □, A, A, Ȧ, A, A, A, □, □, □, □, 𝐀, 𝐴, 𝑨, 𝒜, 𝓐, 𝔄, 𝔸, 𝕬, 𝖠, 𝗔, 𝘈, 𝘼, 𝙰, 𝚨, 𝛢, 𝜜, 𝝖, 𝞐, □, ª,

b b, □, □, □, B, □, B, B, B, ʙ, B, □, □, □, □, □, □

c c, c, □, ċ, □, □, □, C, □, C, C, □, ⊂, ℂ, ℭ, □, □, □, □, □, □, □, □

d d, □, □, □, □, □, D, D, D, D, □, □, □, □, □, □

e e, e, ẹ, ė, é, è, □, □, E, E, E, E, □, □, □, □, □, □, □, □

f f, □, F, □, F, ℱ, □, □, □, □, □, □

g g, ġ, □, g, □, □, ǵ, □, G, □, □, □, □, □, g, ģ, □

h h, һ, □, H, H, H, H, h, ℋ, ℌ, □, □, □

i i, i, í, ï, □, □, I, □, □, □, ǀ, ι, □, □, l, ι, □, □, □, □

j j, j, □, □, □, J, J, □, □, □, □

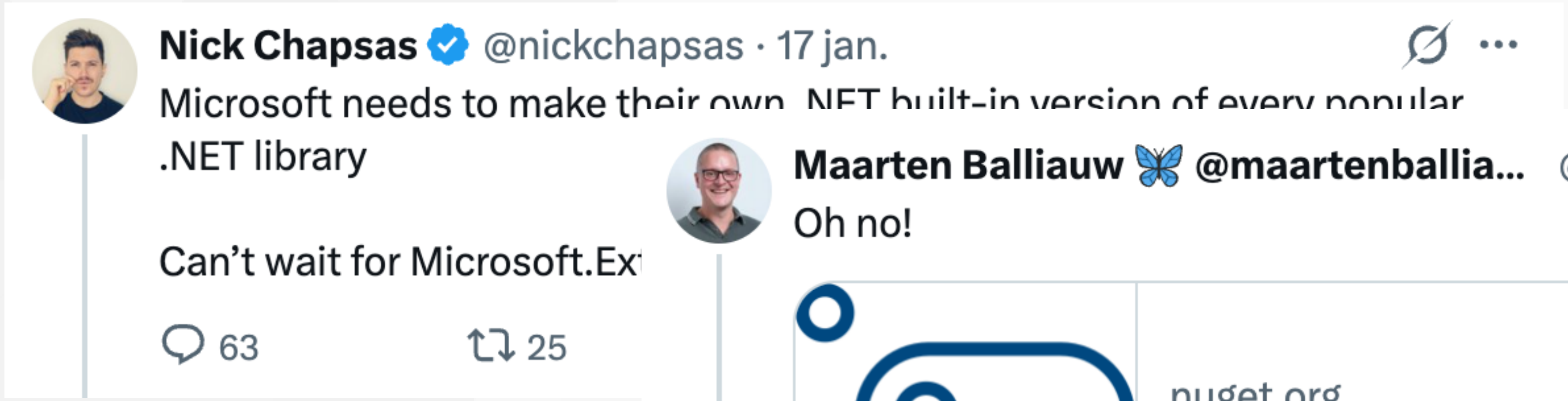
k k, κ, □, K, K, K, □, □, □, □, □, κ, □

l l, □, □, □, L, □, □, ℓ, |, ı, □, □, □, □

m m, □, M, M, M, □, □, □, □, □, □, □, □, □

Duende.

Early 2025…



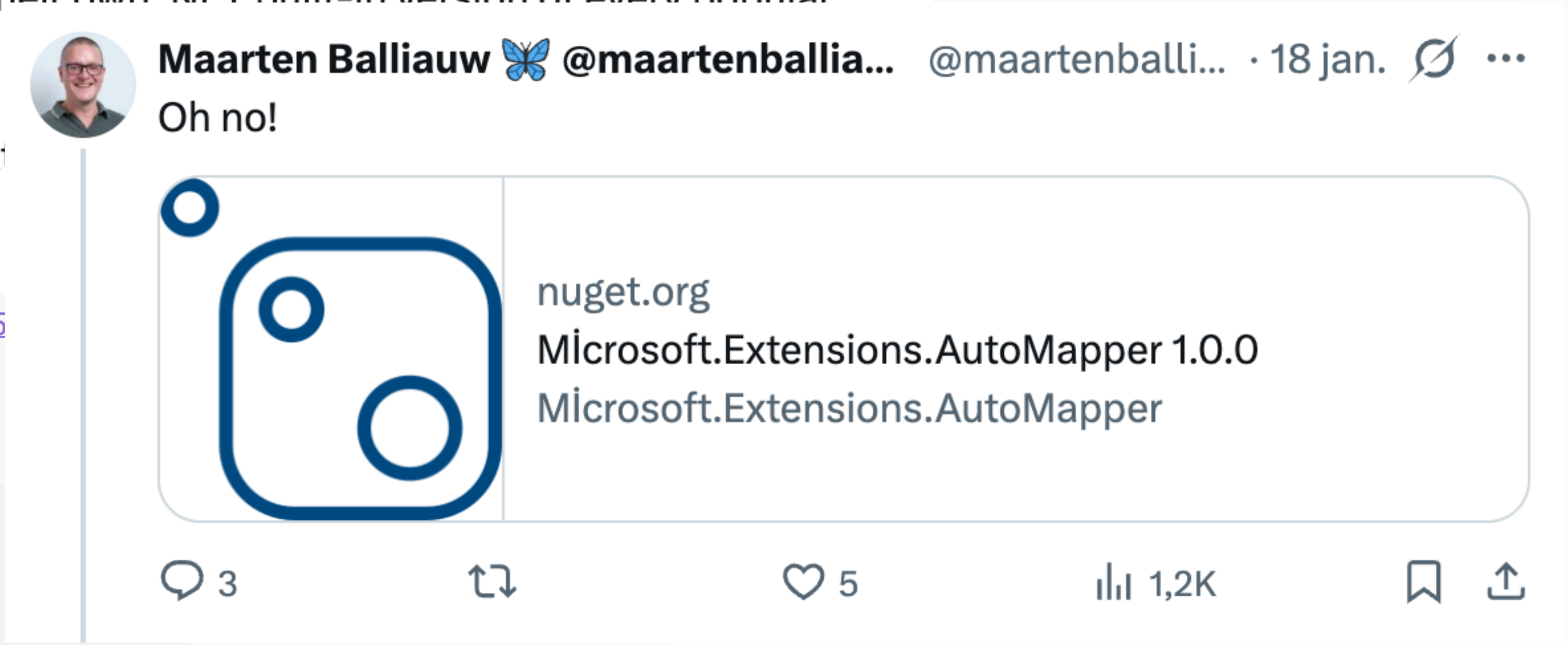
Nick Chapsas @nickchapsas · 17 jan.

Microsoft needs to make their own .NET built-in version of every popular .NET library

Can't wait for Microsoft.Ext

63 25

https://x.com/nickchapsas/status/1880205



Maarten Balliauw 🦋 @maartenballia... @maartenballi... · 18 jan.

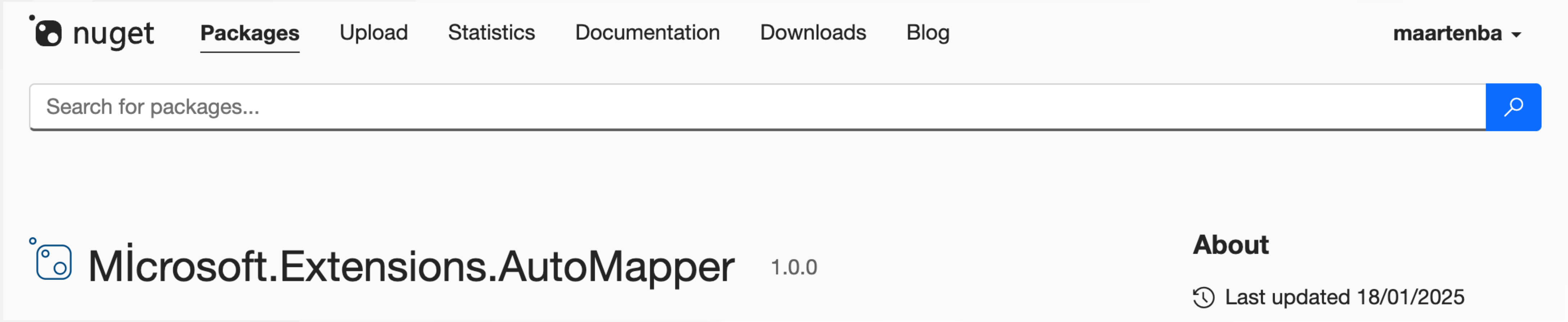
Oh no!

nuget.org
Microsoft.Extensions.AutoMapper 1.0.0
Microsoft.Extensions.AutoMapper

3 5 1,2K

Duende.

Early 2025...



nuget Packages Upload Statistics Documentation Downloads Blog maartenba

Search for packages...

Mİcrosoft.Extensions.AutoMapper 1.0.0

About

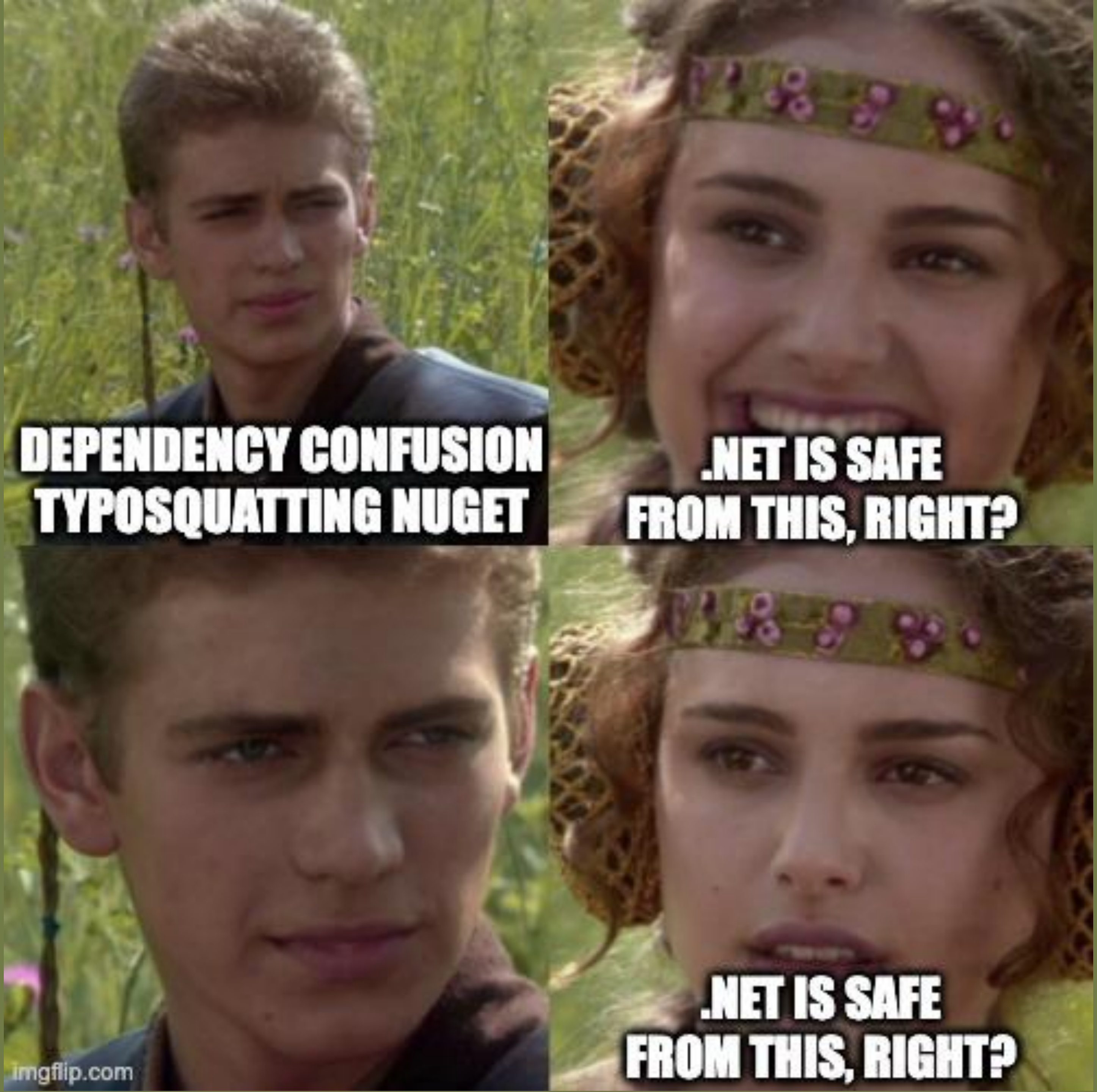
Last updated 18/01/2025

https://www.nuget.org/packages/Mİcrosoft.Extensions.AutoMapper/

Duende.

Early 2025…

- Deleted package
- Contacted NuGet team, not considered for bug bounty
- They refined the configuration of the `TypoSquattingService`
  https://github.com/NuGet/NuGetGallery/blob/main/src/NuGetGallery/Services/TyposquattingService.cs


DEPENDENCY CONFUSION
TYPOSQUATTING NUGET
.NET IS SAFE FROM THIS, RIGHT?
imgflip.com
.NET IS SAFE FROM THIS, RIGHT?

Duende.

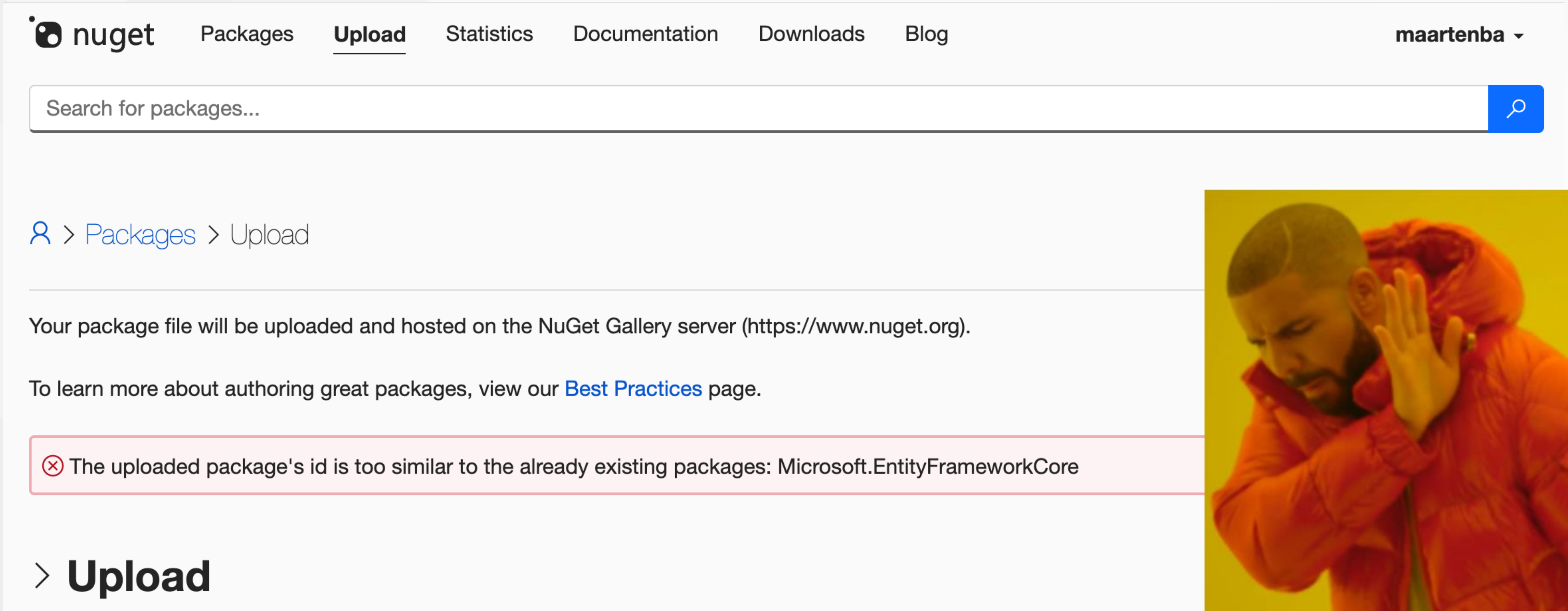
End of 2025, preparing this talk...

```
<Project Sdk="Microsoft.NET.Sdk">

    <PropertyGroup>
        <TargetFramework>net10.0</TargetFramework>
        <ImplicitUsings>enable</ImplicitUsings>
        <Nullable>enable</Nullable>
        <GeneratePackageOnBuild>true</GeneratePackageOnBuild>

        <Version>10.0.0</Version>
        <Title>Microsoft.EntityFrameworkCore</Title>
        <Authors>Microsoft</Authors>
        <Description>Entity Framework Core is a modern object-database mapper for
.NET. It supports LINQ queries, change tracking, updates, and schema migrations.
EF Core works with SQL Server, Azure SQL Database, SQLite, Azure Cosmos DB, MySQL,
PostgreSQL, and other databases through a provider plugin API.
```

End of 2025, preparing this talk...



Packages > Upload

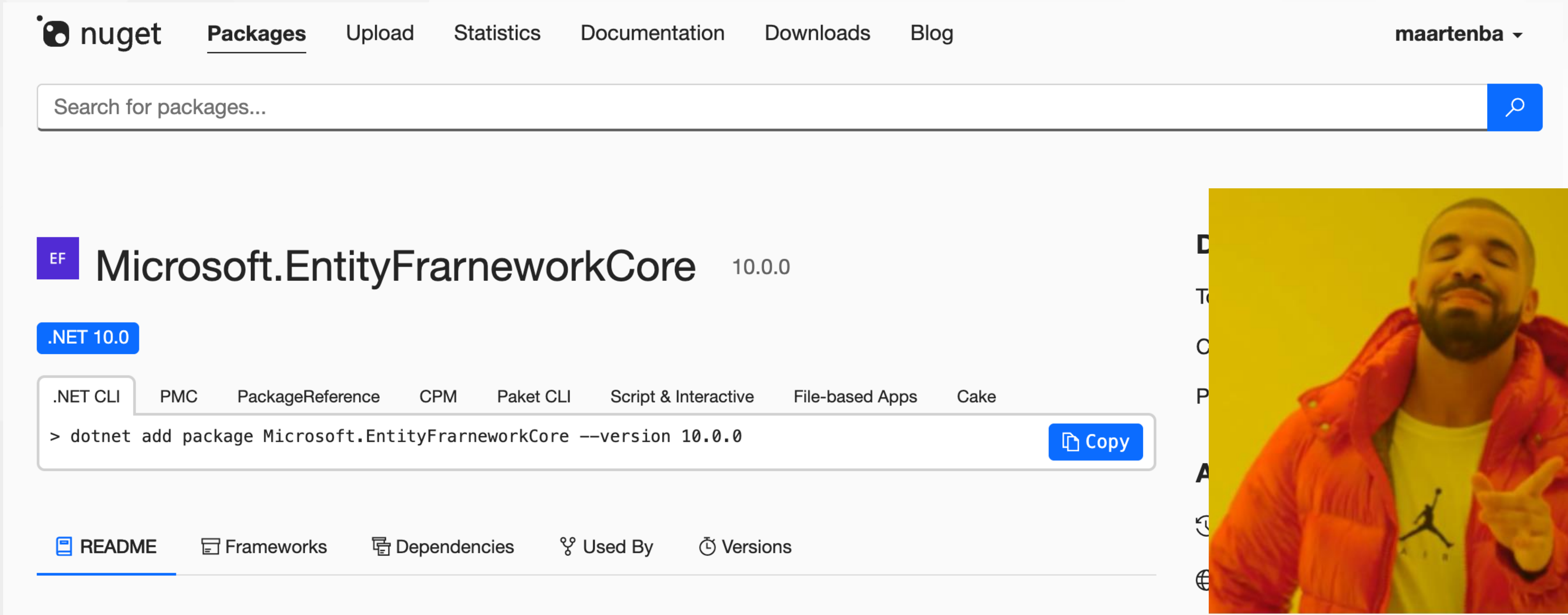
Your package file will be uploaded and hosted on the NuGet Gallery server (https://www.nuget.org).

To learn more about authoring great packages, view our Best Practices page.

The uploaded package's id is too similar to the already existing packages: Microsoft.EntityFrameworkCore

Duende.

End of 2025, preparing this talk...



nuget Packages Upload Statistics Documentation Downloads Blog maartenba

Search for packages...

EF Microsoft.EntityFrarneworkCore 10.0.0

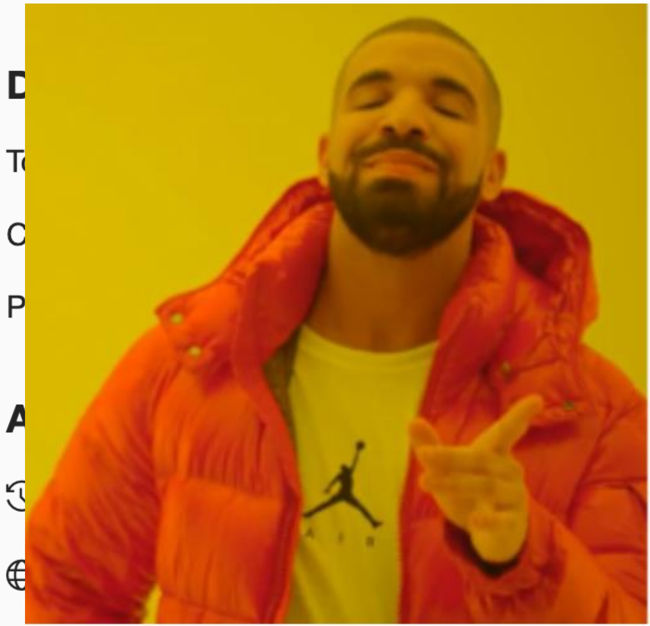
.NET 10.0

.NET CLI | PMC | PackageReference | CPM | Paket CLI | Script & Interactive | File-based Apps | Cake

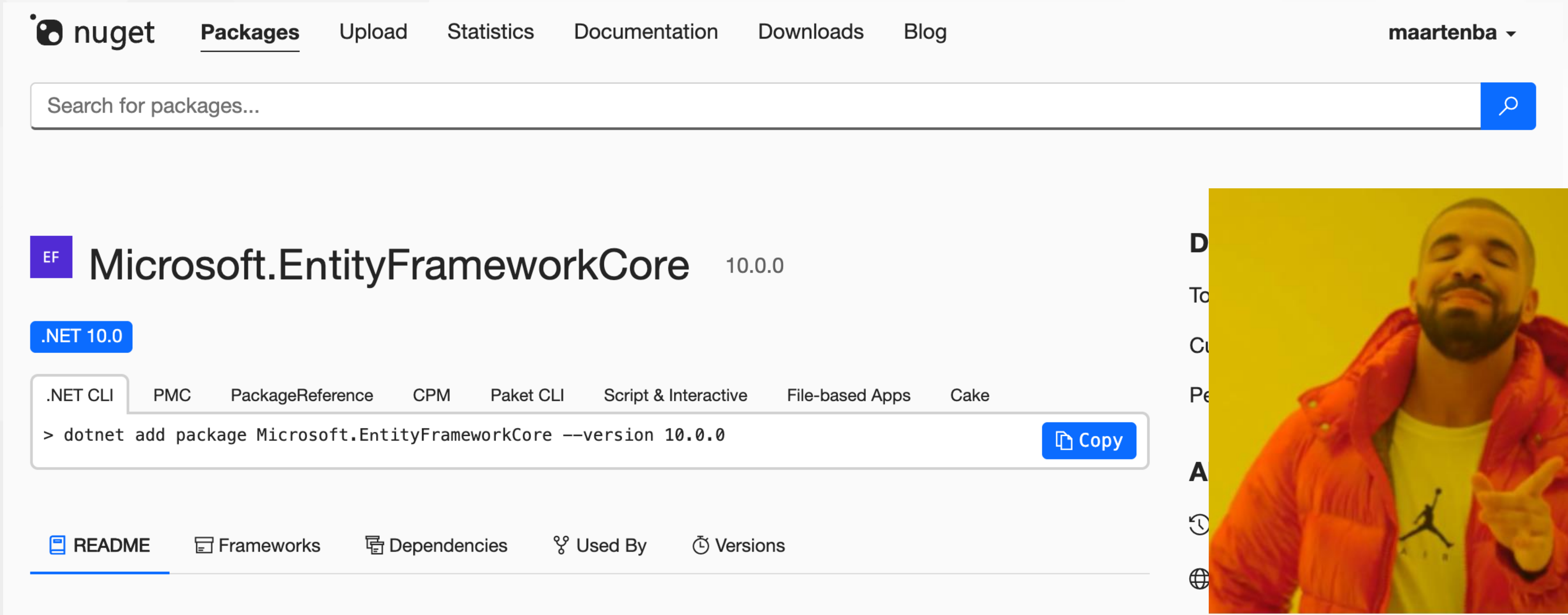
```
> dotnet add package Microsoft.EntityFrarneworkCore --version 10.0.0
```

Copy

README | Frameworks | Dependencies | Used By | Versions



End of 2025, preparing this talk...


nuget Packages Upload Statistics Documentation Downloads Blog maartenba

Search for packages...

Microsoft.EntityFrameworkCore 10.0.0

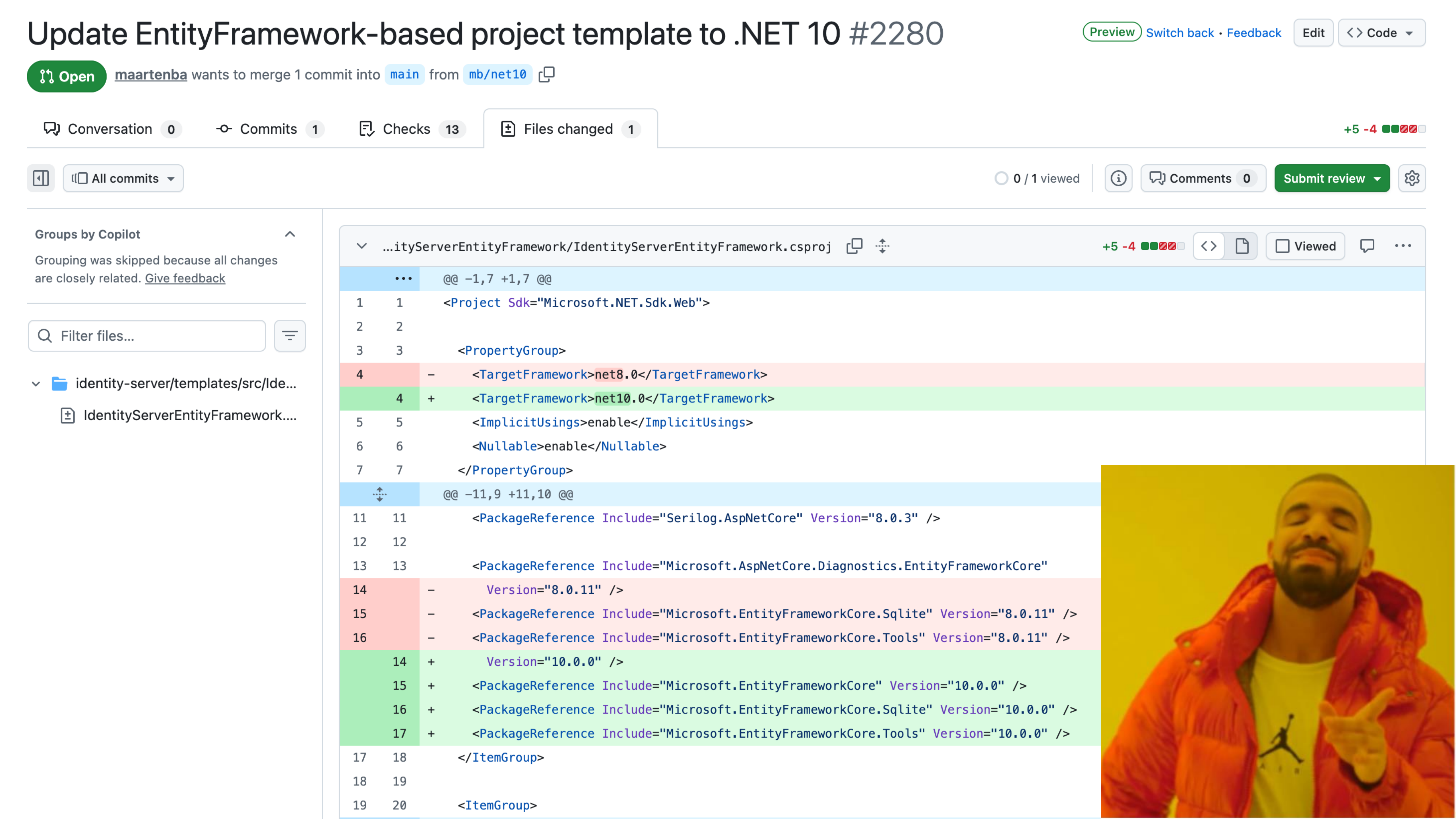
.NET 10.0

.NET CLI PMC PackageReference CPM Paket CLI Script & Interactive File-based Apps Cake

```
> dotnet add package Microsoft.EntityFrameworkCore --version 10.0.0
```

Copy

README Frameworks Dependencies Used By Versions



Update EntityFramework-based project template to .NET 10 #2280

Open maartenba wants to merge 1 commit into `main` from `mb/net10`

Groups by Copilot

Grouping was skipped because all changes are closely related. Give feedback

Filter files...
identity-server/templates/src/Ide...
IdentityServerEntityFramework....
Viewed

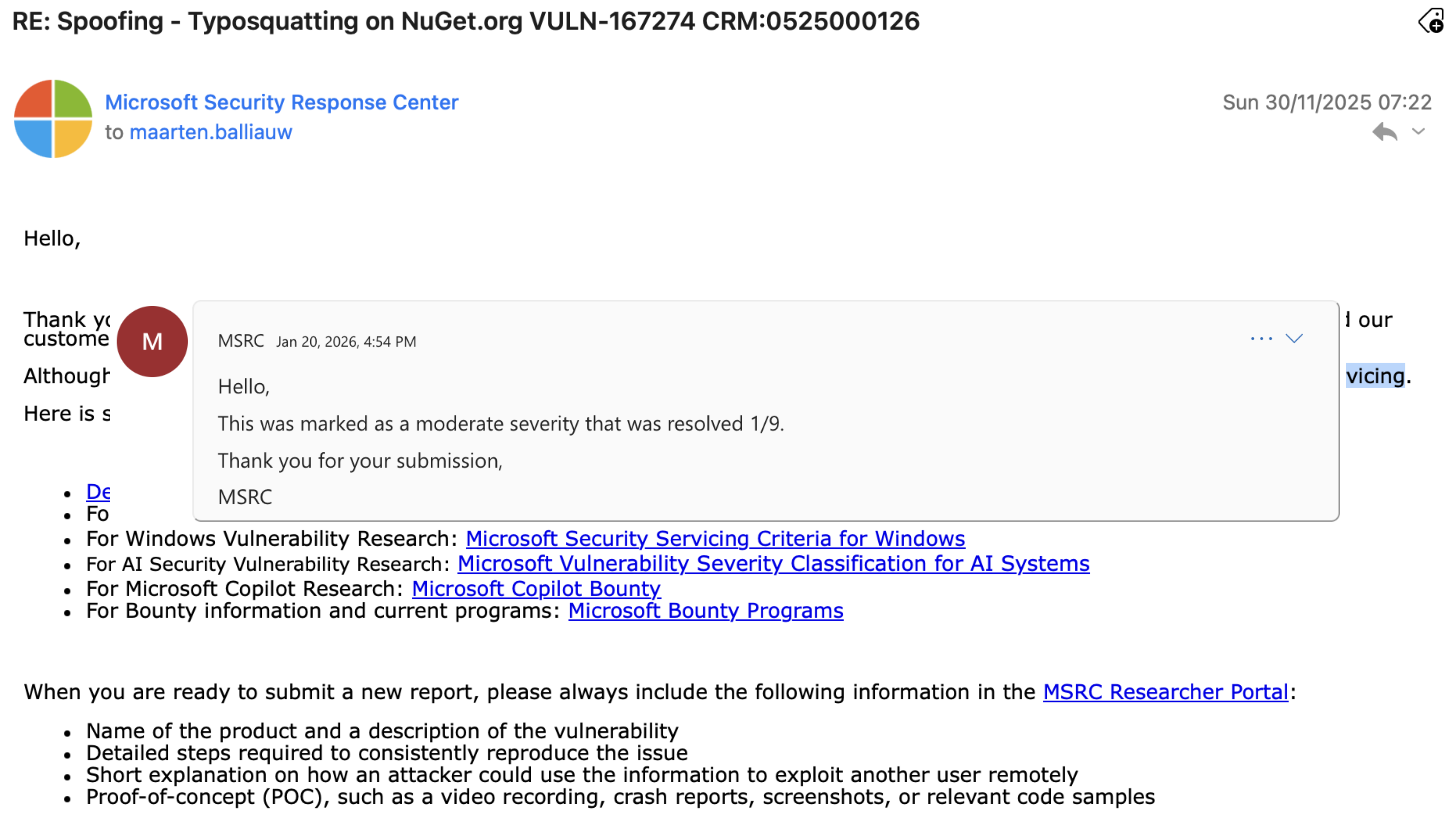
…ityServerEntityFramework/IdentityServerEntityFramework.csproj +5 -4

```
@@ -1,7 +1,7 @@
 <Project Sdk="Microsoft.NET.Sdk.Web">

   <PropertyGroup>
-    <TargetFramework>net8.0</TargetFramework>
+    <TargetFramework>net10.0</TargetFramework>
     <ImplicitUsings>enable</ImplicitUsings>
     <Nullable>enable</Nullable>
   </PropertyGroup>
@@ -11,9 +11,10 @@
     <PackageReference Include="Serilog.AspNetCore" Version="8.0.3" />

     <PackageReference Include="Microsoft.AspNetCore.Diagnostics.EntityFrameworkCore"
-      Version="8.0.11" />
-    <PackageReference Include="Microsoft.EntityFrameworkCore.Sqlite" Version="8.0.11" />
-    <PackageReference Include="Microsoft.EntityFrameworkCore.Tools" Version="8.0.11" />
+      Version="10.0.0" />
+    <PackageReference Include="Microsoft.EntityFrameworkCore" Version="10.0.0" />
+    <PackageReference Include="Microsoft.EntityFrameworkCore.Sqlite" Version="10.0.0" />
+    <PackageReference Include="Microsoft.EntityFrameworkCore.Tools" Version="10.0.0" />
   </ItemGroup>

   <ItemGroup>
```



RE: Spoofing - Typosquatting on NuGet.org VULN-167274 CRM:0525000126

Microsoft Security Response Center
to maarten.balliauw

Sun 30/11/2025 07:22

Hello,

Thank yo ... d our
custome

Althoug ... vicing.

Here is s

MSRC Jan 20, 2026, 4:54 PM

Hello,

This was marked as a moderate severity that was resolved 1/9.

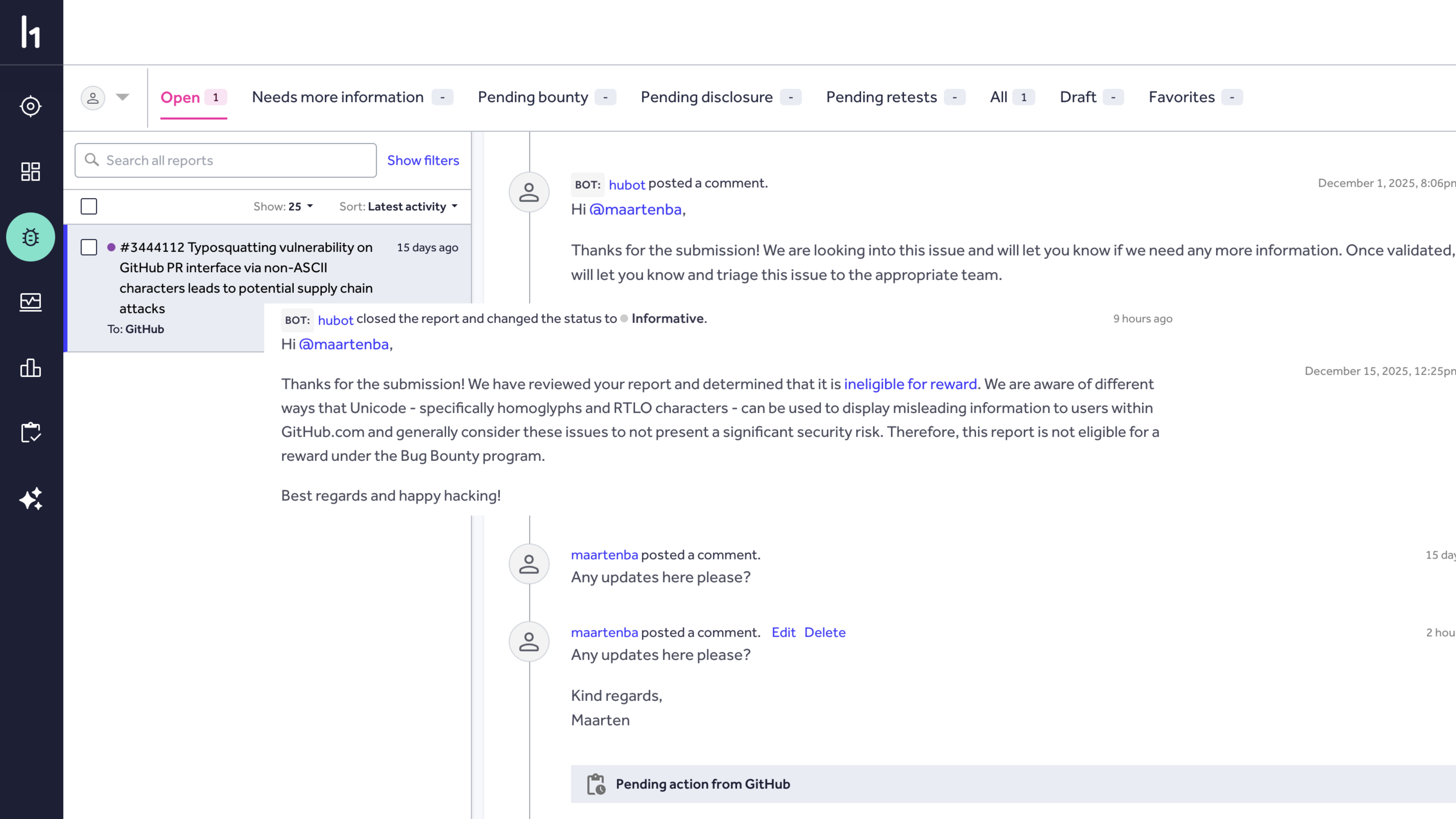
Thank you for your submission,

MSRC

- De
- Fo
- For Windows Vulnerability Research: Microsoft Security Servicing Criteria for Windows
- For AI Security Vulnerability Research: Microsoft Vulnerability Severity Classification for AI Systems
- For Microsoft Copilot Research: Microsoft Copilot Bounty
- For Bounty information and current programs: Microsoft Bounty Programs

When you are ready to submit a new report, please always include the following information in the MSRC Researcher Portal:

- Name of the product and a description of the vulnerability
- Detailed steps required to consistently reproduce the issue
- Short explanation on how an attacker could use the information to exploit another user remotely
- Proof-of-concept (POC), such as a video recording, crash reports, screenshots, or relevant code samples



Open 1 | Needs more information - | Pending bounty - | Pending disclosure - | Pending retests - | All 1 | Draft - | Favorites -

Search all reports Show filters

Show: 25 Sort: Latest activity

#3444112 Typosquatting vulnerability on GitHub PR interface via non-ASCII characters leads to potential supply chain attacks 15 days ago
To: GitHub

BOT: hubot posted a comment. December 1, 2025, 8:06pm

Hi @maartenba,

Thanks for the submission! We are looking into this issue and will let you know if we need any more information. Once validated, will let you know and triage this issue to the appropriate team.

BOT: hubot closed the report and changed the status to ● **Informative**. 9 hours ago

Hi @maartenba,

December 15, 2025, 12:25pm

Thanks for the submission! We have reviewed your report and determined that it is ineligible for reward. We are aware of different ways that Unicode - specifically homoglyphs and RTLO characters - can be used to display misleading information to users within GitHub.com and generally consider these issues to not present a significant security risk. Therefore, this report is not eligible for a reward under the Bug Bounty program.

Best regards and happy hacking!

maartenba posted a comment. 15 day

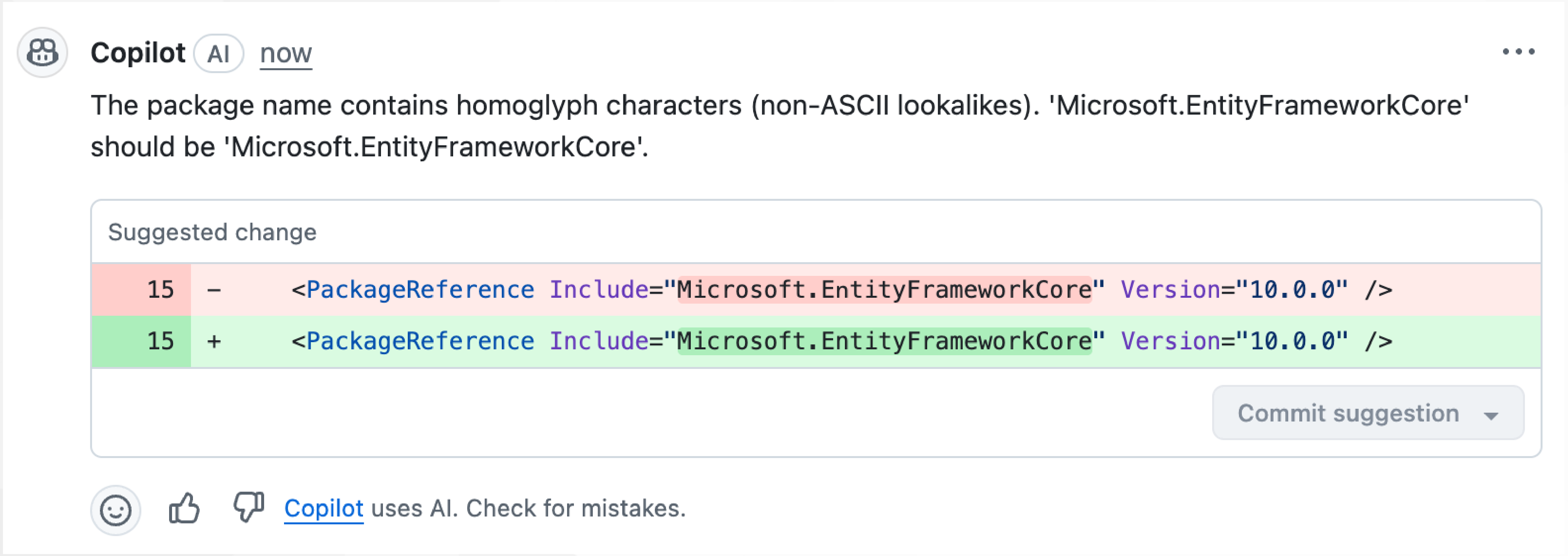
Any updates here please?

maartenba posted a comment. Edit Delete 2 hou

Any updates here please?

Kind regards,
Maarten

Pending action from GitHub



Copilot AI now

The package name contains homoglyph characters (non-ASCII lookalikes). 'Microsoft.EntityFrameworkCore' should be 'Microsoft.EntityFrameworkCore'.

Suggested change

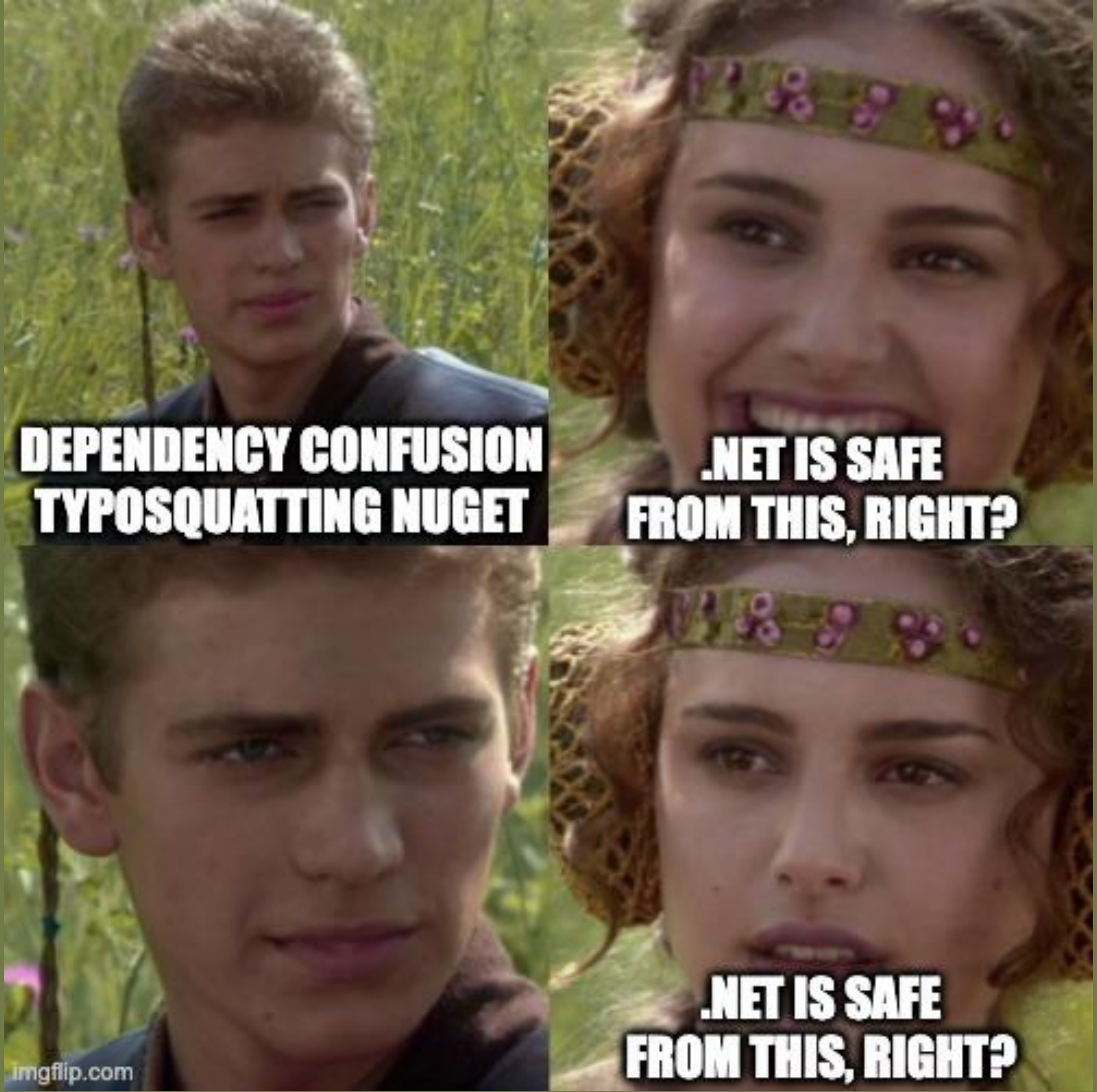
```
15 -     <PackageReference Include="Microsoft.EntityFrameworkCore" Version="10.0.0" />
15 +     <PackageReference Include="Microsoft.EntityFrameworkCore" Version="10.0.0" />
```

Copilot uses AI. Check for mistakes.

Duende.

Typosquatting mitigations

- **Be rigorous in checking pull requests and validating changes**
  - Have @copilot review as well
- **Use package source mapping / package signing**
- `RestorePackagesWithLockFile` **+** `RestoreLockedMode` **on CI**
- **Use [Software Bill of Materials] and analysis tools**


DEPENDENCY CONFUSION TYPOSQUATTING NUGET
.NET IS SAFE FROM THIS, RIGHT?
.NET IS SAFE FROM THIS, RIGHT?
imgflip.com

Duende.

Dropper

Duende.

Dropper

- Install malicious code/payload
- Ideally as close to the NuGet package install as possible
- Ideally goes undetected

Duende.

DEMO

Module Initializers

Duende.

ModuleInitializerAttribute

- Run code when module is initialized

https://learn.microsoft.com/en-us/dotnet/api/system.runtime.compilerservices.moduleinitializerattribute

```
public static class PolicyDiscoveryManager
{
    [ModuleInitializer]
    public static void Manage()
    {
        Console.WriteLine("👻 Spooky!");
    }
}
```

Duende.

More attributes!

- `[EditorBrowsable(EditorBrowsableState.Never)]`
  - *Try* to hide the class in code completion
- `[CompilerGenerated]`
  - Exclude the class from code analysis tooling
- `[DebuggerHidden]`
  - Hint to debugger tools that the class/method can be skipped
- `[DebuggerNonUserCode]`
  - Hint to debugger this is not user code (thanks, Just My Code debugging)

Duende.

DEMO

Source Generators

Duende.

Source generators

- `ModuleInitializerAttribute` is helpful, but in a library need loading
- Generate source code to be part of executing assembly?
- Do things as part of source generation

https://devblogs.microsoft.com/dotnet/introducing-c-source-generators/

Duende.

Source generators - Mitigation

- In your IDE, inspect source generator output
- Use `EmitCompilerGeneratedFiles` build property
- Not airtight: source generator can still run code

Duende.

DEMO

MSBuild

Duende.

NuGet .targets/.props

- Add MSBuild targets or properties by convention
- Write additional files, run processes, …

```
<Project xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
    <PropertyGroup>
        <GeneratedText><![CDATA[C# code goes here...]]></GeneratedText>
    </PropertyGroup>

    <Target Name="AddGeneratedFile" BeforeTargets="BeforeCompile;CoreCompile" Inputs="$(MSBuildAllProjects)"
Outputs="$(IntermediateOutputPath)GeneratedFile.cs">
        <PropertyGroup>
            <GeneratedFilePath>$(IntermediateOutputPath)GeneratedFile.cs</GeneratedFilePath>
        </PropertyGroup>
        <ItemGroup>
            <Compile Include="$(GeneratedFilePath)" />
            <FileWrites Include="$(GeneratedFilePath)" />
        </ItemGroup>
        <WriteLinesToFile Lines="$(GeneratedText)" File="$(GeneratedFilePath)" WriteOnlyWhenDifferent="true" Overwrite="true" />
    </Target>
</Project>
```

Duende.

NuGet `.targets/.props` - Mitigation

- Review imported targets/props in IDE
- No real way to “block”, would disable a lot of core functionality

Duende.

DEMO

Startup Hooks

Duende.

DOTNET_STARTUP_HOOKS

- Run code before a .NET application `Main`
- Based on environment variable

```
public static class StartupHook
{
    public static void Initialize()
    {
        Console.WriteLine("Hello from injected code!");
        Console.SetOut(new InvertedTextWriter(Console.Out));
    }
}
```

Duende.

Other places that can run code in dev workflow

- Source-only NuGet packages + hiding in IDE (not as stealthy)
  https://andrewlock.net/creating-source-only-nuget-packages/
- IDE plugins
- User profile on macOS/Linux
- GitHub Actions (pin them!)
- npm packages
- AI agents? MCP servers?
- Non-user mode (registry, system environment variables, …)

Duende.

Payload

Duende.

Stealth

- Lightweight
- Obfuscate code
- Hide as base64, encrypted code, or Unicode invisible characters
- Steganography
- Terminate research tools
- ...

Duende.

Payload – What do you want to do?

- Harvest credentials **(NuGet, npm, K8s, cloud, GitHub, environment variables, …)**
- Cryptocurrency wallet drains
- Harvest data from well-known locations
- Ransomware
- Damage
- Deploy a SOCKS proxy, remote desktop, …
- Replicate/propagate dropper
- Creative combinations

Duende.

Command and Control (C2)

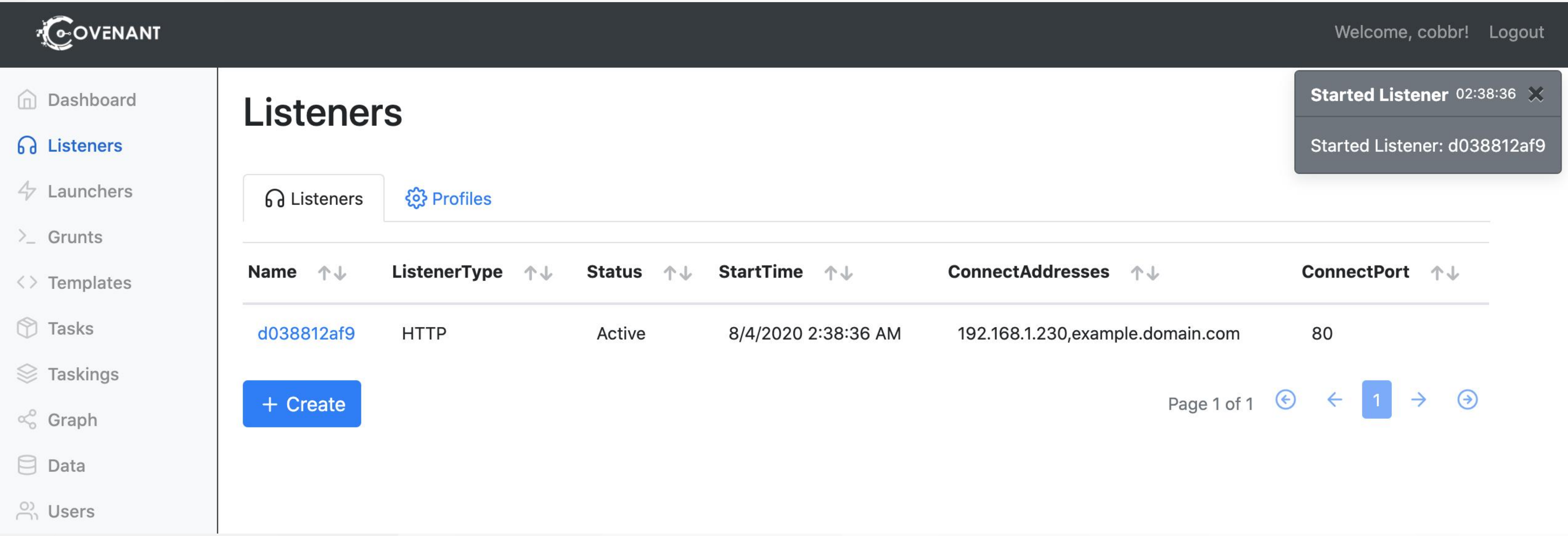
Duende.

Command and Control (C2)

- **A place to phone home**
- **As stealthy as possible**
  - HTTP (custom server, GitHub, public Google Calendar, OneDrive, …)
  - DNS
  - ICMP (e.g. ping and message fields)
  - Blockchain (e.g. Solana memo field)

Covenant

- https://github.com/cobbr/Covenant
- *“Covenant is a .NET command and control framework that aims to highlight the attack surface of .NET”*

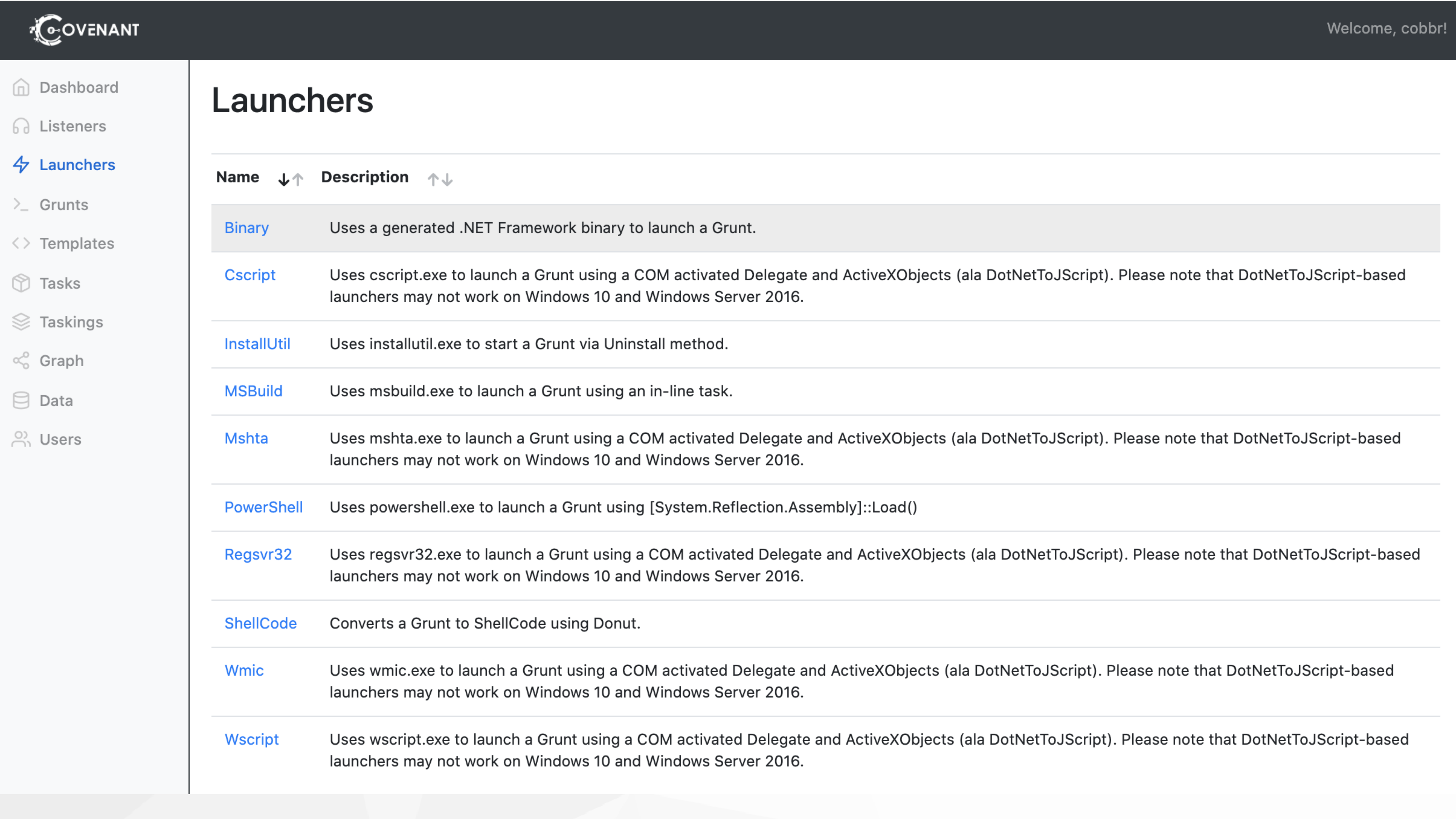


Listeners

Started Listener 02:38:36

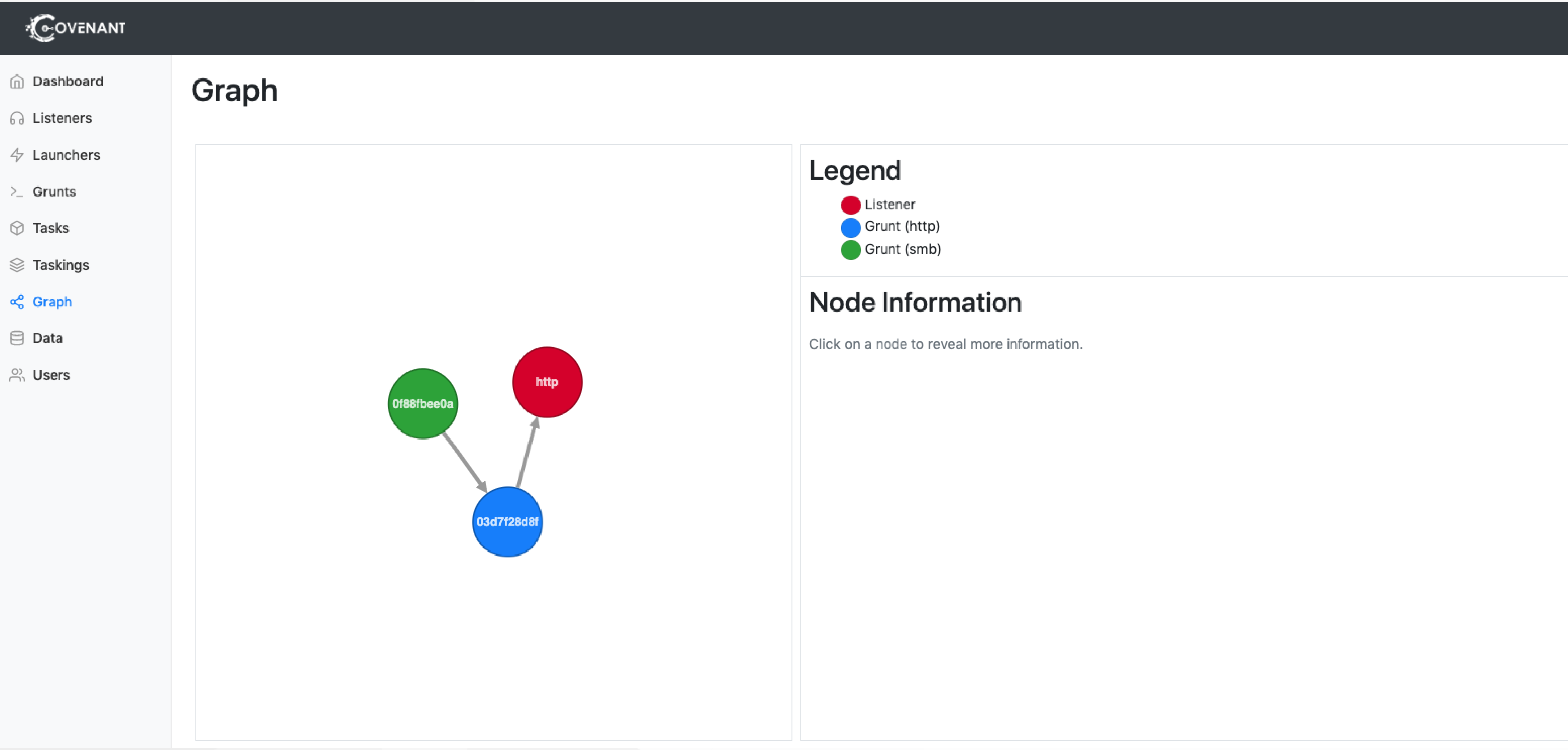
Started Listener: d038812af9

Name	ListenerType	Status	StartTime	ConnectAddresses	ConnectPort
d038812af9	HTTP	Active	8/4/2020 2:38:36 AM	192.168.1.230,example.domain.com	80



Launchers

Name	Description
Binary	Uses a generated .NET Framework binary to launch a Grunt.
Cscript	Uses cscript.exe to launch a Grunt using a COM activated Delegate and ActiveXObjects (ala DotNetToJScript). Please note that DotNetToJScript-based launchers may not work on Windows 10 and Windows Server 2016.
InstallUtil	Uses installutil.exe to start a Grunt via Uninstall method.
MSBuild	Uses msbuild.exe to launch a Grunt using an in-line task.
Mshta	Uses mshta.exe to launch a Grunt using a COM activated Delegate and ActiveXObjects (ala DotNetToJScript). Please note that DotNetToJScript-based launchers may not work on Windows 10 and Windows Server 2016.
PowerShell	Uses powershell.exe to launch a Grunt using [System.Reflection.Assembly]::Load()
Regsvr32	Uses regsvr32.exe to launch a Grunt using a COM activated Delegate and ActiveXObjects (ala DotNetToJScript). Please note that DotNetToJScript-based launchers may not work on Windows 10 and Windows Server 2016.
ShellCode	Converts a Grunt to ShellCode using Donut.
Wmic	Uses wmic.exe to launch a Grunt using a COM activated Delegate and ActiveXObjects (ala DotNetToJScript). Please note that DotNetToJScript-based launchers may not work on Windows 10 and Windows Server 2016.
Wscript	Uses wscript.exe to launch a Grunt using a COM activated Delegate and ActiveXObjects (ala DotNetToJScript). Please note that DotNetToJScript-based launchers may not work on Windows 10 and Windows Server 2016.



Graph

Legend

● Listener
● Grunt (http)
● Grunt (smb)

Node Information

Click on a node to reveal more information.

Duende.

What can you do to mitigate?

Duende.

What can *you* do?

- Explore the various tools and practices in NuGet, GitHub, …
- Rigorous pull request reviews
- Code/dependency analysis tools like Trivy, Aikido Security, Snyk, …
- Endpoint detection tools to prevent environment variable change, DNS, …
- If you see something suspicious, dig in. Better safe than sorry!
  - https://medium.com/@projectcsework/andres-freund-the-man-who-saved-internet-b9de192c63e9

Duende.

Swiss Cheese model

- **Every product has a supply chain, and quality assurance in many steps.**
  - E.g. box of breakfast cereal
- **Your supply chain has checks already**
  - CVE warnings in NuGet, GitHub security scanning, …
  - Package signing, assembly signature, lock files, …
- **You!**

Duende.

Thank you!

duendesoftware.com

Maarten Balliauw
Bluesky: @maartenballiauw.be