



Automating Monthly .NET Patching with GitHub Actions and dotnet-outdated



Martin Costello

Principal Engineer @ Just Eat Takeaway.com
He/him/his




@martin_costello



@martincostello





- .NET Patching and Support Policy 
- The Problem 
- Automate the humans away! 
 - GitHub Actions
 - Update .NET SDK Action and .NET release notes
 - dotnet outdated Global Tool
 - GitHub apps
- Q&A





.NET Patching and Support Policy



- Microsoft publishes a new .NET patch release (almost) every month
- Patches are released on the second Tuesday of the month
 - *"Patch Tuesday"*





 | .NET Blog DevBlogs Developer Technology Languages .NET Platform Development Data Development Theme Login 

.NET Blog

Free. Cross-platform. Open source. A developer platform for building all your apps.


Maintenance & Updates - .NET Blog








.NET April 2023 Updates – .NET 7.0.5, .NET 6.0.16

April 11, 2023

 Rahul Bhandari (MSFT)

Check out April 2023 updates for .NET 7.0. and .NET 6.0

 2 |  0 | .NET .NET Core Maintenance & Updates



.NET March 2023 Updates – .NET 7.0.4, .NET 6.0.15

devblogs.microsoft.com/dotnet



dotnet / announcements

Q Type [f] to search

>_

+



<> Code Issues 219 Pull requests Security Insights

Filters

Q is:open label:Patch-Tuesday

Labels 30

Milestones 3

New issue

✕ Clear current search query, filters, and sorts

63 Open ✓ 0 Closed

Author

Label

Projects

Milestones

Assignee

Sort

• .NET April 2023 updates Monthly-Update .NET 6.0 .NET 7.0 Patch-Tuesday Release Security

#249 opened 2 weeks ago by rbhanda

• .NET March 2023 Updates Monthly-Update .NET 6.0 .NET 7.0 Patch-Tuesday

#248 opened on Mar 14 by rbhanda

• .NET February 2023 Updates Monthly-Update .NET 6.0 .NET 7.0 Patch-Tuesday Security

#246 opened on Feb 14 by rbhanda

• .NET January 2023 Updates Monthly-Update .NET 6.0 .NET 7.0 Patch-Tuesday

#245 opened on Jan 10 by rbhanda

github.com/dotnet/announcements



- ~80% of monthly patches include security fixes
 - [21 of 27](#) .NET 6 releases to March 2024
 - 2 of 2 .NET 8 releases to March 2024
- Recent patched vulnerabilities include:
 - [CVE-2024-21386 - Denial of Service](#)
 - [CVE-2024-0057 - Security Feature bypass](#)
 - [CVE-2023-36796 - Remote Code Execution](#)
 - [CVE-2023-36049 - Elevation of Privilege](#)



You need to run the latest patch for support from Microsoft.

*“Updates are cumulative and released as patches, with each update built upon all of the updates that preceded it. **A device needs to install the latest update to remain supported.** Updates may include new features, fixes (security and/or non-security), or a combination of both.”*

[.NET and .NET Core Support Policy](#)



The problem 🙄



- Every application needs patching every month
 - Keep ahead of bad actors
 - Stay supported
- We only have so much engineering time
- Manual patching doesn't scale
- [Automated Updates](#) only apply to a subset of use cases
- Patching is repetitive
- Patching is **boring**



- Every application needs patching every month
 - Keep ahead of bad actors
 - Stay supported
- We only have so much engineering time
- Manual patching doesn't scale
- [Automated Updates](#) only apply to a subset of use cases
- Patching is repetitive
- Patching is **boring**





Homer Simpson - "Trash of the Titans" S9E22



Automate the humans away! 



Solution

- Create a scheduled, automated GitHub Actions workflow
- Use open source tools to patch our repository
 - update-dotnet-sdk GitHub Action
 - dotnet outdated global tool
- Use GitHub apps to approve and merge the changes
- No extra code needs to be deployed to manage the process



GitHub Actions Workflow

- Just 17 lines of YAML
- Runs weekly on a Cron schedule
- Can be run on-demand
- Uses a [reusable workflow](#)
- Minimal configuration

```
name: update-dotnet-sdk

on:

  schedule:
    - cron: '00 21 * * TUE'

  workflow_dispatch:

permissions:
  contents: read

jobs:
  update-sdk:
    uses: martincostello/update-dotnet-sdk/.github/workflows/update-dotnet-sdk.yml@v2
    with:
      labels: "dependencies,.NET"
      user-email: ${vars.GIT_COMMIT_USER_EMAIL}
      user-name: ${vars.GIT_COMMIT_USER_NAME}
    secrets:
      application-id: ${secrets.UPDATER_APPLICATION_ID}
      application-private-key: ${secrets.UPDATER_APPLICATION_PRIVATE_KEY}
```




GitHub Apps

OAuth Apps

Personal access tokens



GitHub Apps

New GitHub App

**costellobot**

An automation app for [Martin Costell...

Edit

**dotnet-patch-automation-reviewer**

An automation app for the [dotnet-pat...

Edit

**dotnet-patch-automation-updater**

An automation app for the [dotnet-pat...

Edit

A GitHub App can act on its own behalf, taking actions via the API directly instead of impersonating a user. Read more in our [developer documentation](#).

[Developer Settings](#)
[Creating a GitHub app](#)



Permissions

User permissions are granted on an individual user basis as part of the [User authorization flow](#).
Read our [permissions documentation](#) for information about specific permissions.

Changes to permissions will be applied to all future installations. Current users will be prompted to accept any changes and enable the new permissions on their installation.

Repository permissions 3 Selected

Repository permissions permit access to repositories and related resources.



[Creating a GitHub app](#)



Contents ⓘ

Repository contents, commits, branches, downloads, releases, and merges.

Access: Read and write ▼

Pull requests ⓘ

Pull requests and related comments, assignees, labels, milestones, and merges.

Access: Read and write ▼

[Creating a GitHub app](#)



Private keys

[Generate a private key](#)

You need a private key to sign access token requests. [Learn more about private keys.](#)



Private

Private key

SHA256: I6B311hY18BuDxIV+F5ugpJbor8Qb5yEcdaLQynZGv8=

Added 6 hours ago by **martincostello**

[Delete](#)

[Creating a GitHub app](#)



Security

Code security and analysis

Deploy keys

Secrets and variables ^

Actions

Codespaces

Dependabot

Integrations

GitHub Apps

Email notifications

Autolink references

Repository secrets

OSSF_SCORECARD_TOKEN	Updated 5 hours ago		
REVIEWER_APPLICATION_ID	Updated 6 hours ago		
REVIEWER_APPLICATION_PRIVATE_KEY	Updated 6 hours ago		
UPDATER_APPLICATION_ID	Updated yesterday		
UPDATER_APPLICATION_PRIVATE_KEY	Updated yesterday		

[Encrypted secrets](#)



martincostello / dotnet-patch-automation-sample

Type to search

[Code](#) [Issues](#) [Pull requests](#) [Actions](#) [Security](#) [Insights](#) [Settings](#)[← update-dotnet-sdk](#)✓ **update-dotnet-sdk #42**

Re-run all jobs

[Summary](#)

Jobs

✓ **update-sdk**

✓ Update .NET SDK

Run details

[Usage](#)[Workflow file](#)**update-sdk / Update .NET SDK**

succeeded 5 hours ago in 28s

Search logs



> ✓ Set up job	2s
> ✓ Validate secrets	0s
> ✓ Generate GitHub application token	1s
> ✓ Assign GitHub token	0s
> ✓ Checkout code	0s
> ✓ Update .NET SDK	3s
> ✓ Setup .NET SDK	0s
> ✓ Update NuGet packages	20s
> ✓ Post Checkout code	0s
> ✓ Complete job	0s

github.com/martincostello/dotnet-patch-automation-sample



martincostello / dotnet-patch-automation-sample

Search: Type to search

<> Code Issues Pull requests Actions Security 2 Insights Settings

Update .NET SDK to 7.0.203 #83

Merged dotnet-patch-aut... merged 2 commits into main from update-dotnet-sdk-7.0.203 5 hours ago

Conversation 0 Commits 2 Checks 4 Files changed 3 +3 -3

dotnet-patch-automation-updater (bot) commented 5 hours ago

Updates the .NET SDK to version `7.0.203`, which also updates the .NET runtime from version `7.0.4` to version `7.0.5`.

This release includes fixes for the following security issue(s):

- CVE-2023-28260

This pull request was auto-generated by GitHub Actions.

Reviewers: **dotnet-patch-automation-reviewer** ✓

Assignees: No one—assign yourself

Labels: **dependencies** **.NET**

Projects: None yet

Milestone: No milestone

Development: Successfully merging this pull request may close these issues. None yet

Notifications: Customize

Unsubscribe

You're receiving notifications because you're watching this repository.

Update .NET SDK ✓ @00a99c

dotnet-patch-automation-updater (bot) added **.NET** **dependencies** labels 5 hours ago

Bump .NET NuGet packages ✓ 5ab39ea

dotnet-patch-automation-reviewer (bot) approved these changes 5 hours ago View reviewed changes

dotnet-patch-automation-reviewer (bot) enabled auto-merge (squash) 5 hours ago

dotnet-patch-automation-reviewer (bot) merged commit `7174d08` into `main` 5 hours ago 4 checks passed View details Revert

github.com/martincostello/dotnet-patch-automation-sample



Showing 3 changed files with 3 additions and 3 deletions.

Split

Unified

Filter changed files

- global.json
- src/ToDoApp
 - ToDoApp.csproj
- tests/ToDoApp.Tests
 - ToDoApp.Tests.csproj

```
2 global.json
... @@ -1,6 +1,6 @@
1 1 {
2 2   "sdk": {
3 -   "version": "7.0.202",
3 +   "version": "7.0.203",
4 4   "allowPrerelease": false,
5 5   "rollForward": "latestMajor"
6 6   }
```

```
2 src/ToDoApp/ToDoApp.csproj
@@ -10,7 +10,7 @@
10 10 </PropertyGroup>
11 11 <ItemGroup>
12 12   <PackageReference Include="AspNet.Security.OAuth.GitHub" Version="7.0.2" />
13 -  <PackageReference Include="Microsoft.EntityFrameworkCore.Sqlite" Version="7.0.4" />
13 +  <PackageReference Include="Microsoft.EntityFrameworkCore.Sqlite" Version="7.0.5" />
14 14   <PackageReference Include="Microsoft.TypeScript.MSBuild" Version="5.0.4" PrivateAssets="all" />
15 15   <PackageReference Include="NodaTime" Version="3.1.9" />
16 16 </ItemGroup>
```

github.com/martincostello/dotnet-patch-automation-sample



How does it work?

[Marketplace](#) / [Actions](#) / Update .NET SDK

GitHub Action

Update .NET SDK

v2.1.2

Latest version

Use latest version

Update .NET SDK

This action updates the .NET SDK version specified by a `global.json` file stored in a GitHub repository.

An example Pull Request created by the action can be found [here](#).

Example Usage

```
steps:
  - uses: actions/checkout@v3
  - uses: martincostello/update-dotnet-sdk@v2
    with:
```

Stars

 Starred 6

Contributors



Categories

Dependency management

Utilities

Links

 [martincostello/update-dotnet-sdk](#) [Open issues](#) 2 [Pull requests](#) 0[Update .NET SDK GitHub Action](#)



Update .NET SDK Action

- JavaScript action
- Checks the [.NET release notes](#)
- Updates global.json
- Uses the GitHub API to create (and label) a pull request

```
- name: Update .NET SDK
  id: update-dotnet-sdk
  uses: martincostello/update-dotnet-sdk@v2
  with:
    branch-name: ${ inputs.branch-name }
    channel: ${ inputs.channel }
    commit-message: ${ inputs.commit-message }
    dry-run: ${ inputs.dry-run }
    global-json-file: ${ inputs.global-json-file }
    labels: ${ inputs.labels }
    repo-token: ${ steps.assign-token.outputs.access-token }
    user-email: ${ inputs.user-email }
    user-name: ${ inputs.user-name }
```



dotnet / core

Type to search

[Code](#) [Issues](#) 409 [Pull requests](#) 14 [Actions](#) [Projects](#) [Security](#) [Insights](#)

Code



main



Go to file



- cve.md
- install-linux.md
- install-macos.md
- install-maui.md
- install-windows.md
- install.md
- known-issues.md
- linux-packages.md
- releases.json
- runtime-deps.json
- supported-os.md

> 7.0

> 8.0

[core / release-notes / 6.0 / releases.json](#)

rbhanda Artifacts for .NET April 2023 Releases (#8381) ✓

2876b2f · 2 weeks ago

[History](#)

Code

Blame

14835 lines (14835 loc) · 1010 KB

Raw



```
1  {
2    "channel-version": "6.0",
3    "latest-release": "6.0.16",
4    "latest-release-date": "2023-04-11",
5    "latest-runtime": "6.0.16",
6    "latest-sdk": "6.0.408",
7    "release-type": "lts",
8    "support-phase": "active",
9    "eol-date": "2024-11-12",
10   "lifecycle-policy": "https://dotnet.microsoft.com/platform/support/policy/",
11   "releases": [
12     {
13       "release-date": "2023-04-11",
14       "release-version": "6.0.16",
15       "security": true,
16       "cve-list": [
17         {
18           "cve-id": "CVE-2023-28260",
19           "cve-url": "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28260"
20         }
21       ]
22     }
23   ]
24 }
```



.NET

Why .NET

Features

Learn

Docs

Downloads

Community

LIVE TV

All Microsoft

Home / Download / .NET / 6.0

Download .NET 6.0

Not sure what to download? [See recommended downloads for the latest version of .NET.](#)

6.0.16 Security patch

[Release notes](#) Latest release date April 11, 2023

Build apps - SDK

SDK 6.0.408

OS	Installers	Binaries
Linux	Package manager instructions	Arm32 Arm32 Alpine Arm64 Arm64 Alpine x64 x64 Alpine
macOS	Arm64 x64	Arm64 x64
Windows	Arm64 x64 x86 x86-x64	Arm64 x64 x86

Run apps - Runtime

ASP.NET Core Runtime 6.0.16

The ASP.NET Core Runtime enables you to run existing web/server applications. On Windows, we recommend installing the Hosting Bundle, which includes the .NET Runtime and IIS support.

IIS runtime support (ASP.NET Core Module v2)

16.0.23083.16



dotnet outdated global tool

- .NET global tool CLI application
- Published via NuGet - [package](#)
- Checks NuGet for package updates
- Supports filtering by package and SemVer tags
- Updates <PackageReference> and <PackageVersion> tags

```
PowerShell Core X + v

dotnet-patch-automation-sample (ca97a99) [!] via .NET v7.0.202
> dotnet outdated
» TodoApp
  [net7.0]
  Microsoft.EntityFrameworkCore.Sqlite 7.0.4 -> 7.0.5

» TodoApp.Tests
  [net7.0]
  Shouldly 4.2.0 -> 4.2.1

Version color legend:
<red> : Major version update or pre-release version. Possible breaking changes.
<yellow>: Minor version update. Backwards-compatible features added.
<green> : Patch version update. Backwards-compatible bug fixes.

You can upgrade packages to the latest version by passing the -u or -u:prompt option.
Elapsed: 00:00:02.9052013

dotnet-patch-automation-sample (ca97a99) [!] via .NET v7.0.202 took 3s
> |
```



dotnet outdated global tool

- .NET global tool CLI application
- Published via NuGet - [package](#)
- Checks NuGet for package updates
- Supports filtering by package and SemVer tags
- Updates <PackageReference> and <PackageVersion> tags

```
PowerShell Core
dotnet-patch-automation-sample (ca97a99) via .NET v7.0.202
> dotnet outdated --upgrade --version-lock Major --include "Microsoft.AspNetCore."
» TodoApp.Tests
  [net7.0]
  Microsoft.AspNetCore.Mvc.Testing 7.0.4 -> 7.0.5

Version color legend:
<red>   : Major version update or pre-release version. Possible breaking changes.
<yellow>: Minor version update. Backwards-compatible features added.
<green> : Patch version update. Backwards-compatible bug fixes.

Upgrading package Microsoft.AspNetCore.Mvc.Testing...
Project TodoApp.Tests [net7.0] upgraded successfully

Elapsed: 00:00:00.3794555

dotnet-patch-automation-sample (ca97a99) [!] via .NET v7.0.202 took 9s
> |
```



dotnet outdated global tool

- .NET global tool CLI application
- Published via NuGet - [package](#)
- Checks NuGet for package updates
- Supports filtering by package and SemVer tags
- Updates `<PackageReference>` and `<PackageVersion>` tags

```
PowerShell Core

dotnet-patch-automation-sample (ca97a99) [!] via .NET v7.0.202
> git diff
diff --git a/tests/ToDoApp.Tests/ToDoApp.Tests.csproj b/tests/ToDoApp.Tests/ToDoApp.Tests.csproj
index 1974f40..3d994ca 100644
--- a/tests/ToDoApp.Tests/ToDoApp.Tests.csproj
+++ b/tests/ToDoApp.Tests/ToDoApp.Tests.csproj
@@ -10,7 +10,7 @@
   <PackageReference Include="GitHubActionsTestLogger" Version="2.0.1" />
   <PackageReference Include="JustEat.HttpClientInterception" Version="4.0.0" />
   <PackageReference Include="MartinCostello.Logging.XUnit" Version="0.3.0" />
-  <PackageReference Include="Microsoft.AspNetCore.Mvc.Testing" Version="7.0.4" />
+  <PackageReference Include="Microsoft.AspNetCore.Mvc.Testing" Version="7.0.5" />
   <PackageReference Include="Microsoft.NET.Test.Sdk" Version="17.5.0" />
   <PackageReference Include="Microsoft.Playwright" Version="1.32.0" />
   <PackageReference Include="ReportGenerator" Version="5.1.19" />

dotnet-patch-automation-sample (ca97a99) [!] via .NET v7.0.202
> |
```




dotnet outdated global tool

- .NET global tool CLI application
- Published via NuGet - [package](#)
- Checks NuGet for package updates
- Supports filtering by package and SemVer tags
- Updates <PackageReference> and <PackageVersion> tags

```
PowerShell Core

dotnet-patch-automation-sample on  main via .NET v7.0.203
> dotnet outdated --upgrade --version-lock Major --include "Microsoft.AspNetCore."
No outdated dependencies were detected
Elapsed: 00:00:03.5705699

dotnet-patch-automation-sample on  main via .NET v7.0.203 took 4s
> |
```

dotnet outdated global tool

- .NET global tool CLI application
- Published via NuGet - [package](#)
- Checks NuGet for package updates
- Supports filtering by package and SemVer tags
- Updates <PackageReference> and <PackageVersion> tags



```
$eligiblePackages = "${ inputs.include-nuget-packages }".Split(',')
$includePackages = @()

foreach ($package in $eligiblePackages) {
    $includePackages += "--include"
    $includePackages += $package
}

dotnet outdated `
    --upgrade `
    --version-lock Major `
    --output $updatesPath `
    $includePackages

$dependencies = @()

if (Test-Path $updatesPath) {
    $dependencies = `
        Get-Content -Path $updatesPath | `
        ConvertFrom-Json | `
        Select-Object -ExpandProperty projects | `
        Select-Object -ExpandProperty TargetFrameworks | `
        Select-Object -ExpandProperty Dependencies | `
        Sort-Object -Property Name -Unique
}
```

dotnet outdated global tool

- .NET global tool CLI application
- Published via NuGet - [package](#)
- Checks NuGet for package updates
- Supports filtering by package and SemVer tags
- Updates <PackageReference> and <PackageVersion> tags

```
$commitLines = @(
$sdkVersion = "${ steps.update-dotnet-sdk.outputs.sdk-version }}"

if ($deps.Count -eq 1) {
    $commitLines += "Bump $($deps[0].Name) from $($deps[0].ResolvedVersion) to $($deps[0].LatestVersion)"
    $commitLines += ""
    $commitLines += "Bumps $($deps[0].Name) from $($deps[0].ResolvedVersion) to $($deps[0].LatestVersion)."
} else {
    $commitLines += "Bump .NET NuGet packages"
    $commitLines += ""
    $commitLines += "Bumps .NET dependencies to their latest versions for the .NET $sdkVersion SDK."
    $commitLines += ""
    foreach ($dep in $deps) {
        $commitLines += "Bumps $($dep.Name) from $($dep.ResolvedVersion) to $($dep.LatestVersion)."
    }
}

$commitLines += ""
$commitLines += "---"
$commitLines += "updated-dependencies:"

foreach ($dep in $deps) {
    $commitLines += "- dependency-name: $($dep.Name)"
    $commitLines += "  dependency-type: direct:production"
    $commitLines += "  update-type: version-update:semver-$(($dep.UpgradeSeverity.ToLowerInvariant()))"
}

$commitLines += "..."
$commitLines += ""
$commitLines += ""

$commitMessage = $commitLines -join "`n"
```



dotnet outdated global tool

- .NET global tool CLI application
- Published via NuGet - [package](#)
- Checks NuGet for package updates
- Supports filtering by package and SemVer tags
- Updates `<PackageReference>` and `<PackageVersion>` tags

✓ Bump Shouldly from 4.2.0 to 4.2.1

Bumps [Shouldly](<https://github.com/shouldly/shouldly>) from 4.2.0 to 4.2.1.

- [Release notes](<https://github.com/shouldly/shouldly/releases>)
- [Changelog](<https://github.com/shouldly/shouldly/blob/master/BREAKING%20CHANGES.txt>)
- [Commits]([shouldly/shouldly@4.2.0...4.2.1](#))

updated-dependencies:

- dependency-name: Shouldly
 dependency-type: direct:production
 update-type: version-update:semver-patch

...

Signed-off-by: dependabot[bot] <support@github.com>



dependabot[bot] committed yesterday

Verified



dotnet outdated global tool

- .NET global tool CLI application
- Published via NuGet - [package](#)
- Checks NuGet for package updates
- Supports filtering by package and SemVer tags
- Updates `<PackageReference>` and `<PackageVersion>` tags

```
Bump .NET NuGet packages
```

```
Bumps .NET dependencies to their latest versions for the .NET 7.0.203 SDK.
```

```
Bumps Microsoft.AspNetCore.Mvc.Testing from 7.0.0 to 7.0.5.
```

```
Bumps Microsoft.EntityFrameworkCore.Sqlite from 7.0.0 to 7.0.5.
```

```
---
```

```
updated-dependencies:
```

```
- dependency-name: Microsoft.AspNetCore.Mvc.Testing
```

```
  dependency-type: direct:production
```

```
  update-type: version-update:semver-patch
```

```
- dependency-name: Microsoft.EntityFrameworkCore.Sqlite
```

```
  dependency-type: direct:production
```

```
  update-type: version-update:semver-patch
```

```
...
```



Approval Workflow

- Uses another GitHub app to approve and auto-merge
- Only runs for PRs from the expected updater GitHub app
- Parses the commit messages to check only the expected changes have been made
- Copies approach from Dependabot's [fetch-metadata](#) action
- Leverages the [GitHub CLI](#) to perform API requests

```
name: approve-and-merge

on:
  pull_request:
    branches: [ main ]

permissions:
  contents: read

jobs:
  review-pull-request:
    runs-on: ubuntu-latest

    if: ${ github.event.pull_request.user.login == vars.GIT_COMMIT_USER_NAME }}
```



← approve-and-merge

✓ Update .NET SDK to 7.0.203 #164

Re-run all jobs



Summary

Jobs

✓ review-pull-request

Run details

Usage

Workflow file

review-pull-request

succeeded 3 hours ago in 24s

Search logs



- > ✓ Set up job 1s
- > ✓ Generate GitHub application token 1s
- > ✓ Install powershell-yaml 13s
- > ✓ Check which dependencies were updated 4s
- > ✓ Checkout code 0s
- > ✓ Approve pull request and enable auto-merge 0s
 - ✓ Disable auto-merge and dismiss approvals 0s
- > ✓ Post Checkout code 0s
- > ✓ Complete job 0s



Approval Workflow

- Uses another GitHub app to approve and auto-merge
- Only runs for PRs from the expected updater GitHub app
- Parses the commit messages to check only the expected changes have been made
- Copies approach from Dependabot's [fetch-metadata](#) action
- Leverages the [GitHub CLI](#) to perform API requests

```
$commits = gh api `
  /repos/${github.repository }}/pulls/${github.event.pull_request.number }/commits `
--jq '.[ ] | { author: .author.login, message: .commit.message }' | ConvertFrom-Json

$expectedUser = "${vars.GIT_COMMIT_USER_NAME}"
$onlyDependencyUpdates = $True
$onlyChangesFromUser = $True

$dependencies = @()

foreach ($commit in $commits) {
  if ($commit.Author -ne $expectedUser) {
    $onlyChangesFromUser = $False
  }
  $match = [Regex]::Match($commit.Message, '(?m)^--{3}\s(?:<dependencies>[\S\s]*)\s^\.{3}$')
  if ($match.Success -eq $True) {
    $metadata = ($match.Value | ConvertFrom-Yaml -Ordered)
    $updates = $metadata["updated-dependencies"]
    if ($updates) {
      foreach ($update in $updates) {
        $dependencies += @{
          Name = $update['dependency-name'];
          Type = $update['update-type'];
        }
      }
    }
  }
  else {
    $onlyDependencyUpdates = $False
  }
}

$isPatch = $dependencies.Length -gt 0
$onlyTrusted = $dependencies.Length -gt 0
$trustedPackages = $env:INCLUDE_NUGET_PACKAGES.Split(',')

foreach ($dependency in $dependencies) {
  $isPatch = $isPatch -And $dependency.Type -eq "version-update:semver-patch"
  $onlyTrusted = $onlyTrusted -And
  (
    ($dependency.Name -eq "Microsoft.NET.Sdk") -Or
    (($trustedPackages | Where-Object { $dependency.Name.StartsWith($_) }).Count -gt 0)
  )
}

$isTrusted = (($onlyTrusted -And $isPatch) -And $onlyChangesFromUser) -And $onlyDependencyUpdates
"is-trusted-update=$isTrusted" >> $env:GITHUB_OUTPUT
```




Approval Workflow

- Uses another GitHub app to approve and auto-merge
- Only runs for PRs from the expected updater GitHub app
- Parses the commit messages to check only the expected changes have been made
- Copies approach from Dependabot's [fetch-metadata](#) action
- Leverages the [GitHub CLI](#) to perform API requests

```
$approvals = gh api /repos/${{ github.repository }}/pulls/${{ github.event.pull_request.number }}/reviews | ConvertFrom-Json
$approvals = $approvals | Where-Object { $_.user.login -eq $env:REVIEWER_LOGIN }
$approvals = $approvals | Where-Object { $_.state -eq "APPROVED" }



if ($approvals.Length -eq 0) {
  gh pr checkout "$env:PR_URL"
  gh pr review --approve "$env:PR_URL"
  gh pr merge --auto --squash "$env:PR_URL"
}
else {
  Write-Host "PR already approved.";
}
```



  dotnet-patch-automation-reviewer bot approved these changes 53 minutes ago

[View reviewed changes](#)

  dotnet-patch-automation-reviewer bot enabled auto-merge (squash) 53 minutes ago

  dotnet-patch-automation-reviewer bot merged commit **7d413bd** into **main** 48 minutes ago
7 checks passed

[View details](#)

[Revert](#)

  dotnet-patch-automation-reviewer bot deleted the **update-dotnet-sdk-7.0.203** branch 48 minutes ago

[Restore branch](#)

[Pull request](#)





Approval Workflow


- Uses another GitHub app to approve and auto-merge
- Only runs for PRs from the expected updater GitHub app
- Parses the commit messages to check only the expected changes have been made
- Copies approach from Dependabot's [fetch-metadata](#) action
- Leverages the [GitHub CLI](#) to perform API requests


```
$approvals = gh api /repos/${{ github.repository }}/pulls/${{ github.event.pull_request.number }}/reviews | ConvertFrom-Json
$approvals = $approvals | Where-Object { $_.user.login -eq $env:REVIEWER_LOGIN }
$approvals = $approvals | Where-Object { $_.state -eq "APPROVED" }



if ($approvals.Length -gt 0) {
    gh pr checkout "$env:PR_URL"
    gh pr merge --disable-auto "$env:PR_URL"
    foreach ($approval in $approvals) {
        gh api `
            --method PUT `
            /repos/${{ github.repository }}/pulls/${{ github.event.pull_request.number }}/reviews/${$approval.id}/dismissals `
            -f message='Cannot approve as other changes have been introduced.' `
            -f event='DISMISS'
    }
}
else {
    Write-Host "PR not already approved.";
}
```






 **github-actions** bot previously approved these changes last month [View reviewed changes](#)


 **github-actions** bot enabled auto-merge (squash) last month

 **costellobot** and others added 2 commits last month

  Bump .NET NuGet packages ... ✓ 3a8a26b

  Update README ... Verified ✓ adc7ae5

 **github-actions** bot disabled auto-merge last month

 **github-actions** bot dismissed their stale review last month

Cannot approve as other changes have been introduced.

[Pull request](#)



In Summary



- Create two GitHub apps:
 - Updater
 - Reviewer
- Add two workflow files:
 - [Update](#)
 - [Approve and merge](#)
- Wait until Patch Tuesday



- Create two GitHub apps:
 - Updater
 - Reviewer
- Add two workflow files:
 - [Update](#)
 - [Approve and merge](#)
- Wait until Patch Tuesday





Links

- Sample code - [martincostello/dotnet-patch-automation-sample](https://github.com/martincostello/dotnet-patch-automation-sample)
- Update .NET SDK Action - [martincostello/update-dotnet-sdk](https://github.com/martincostello/update-dotnet-sdk)
- .NET Outdated - [dotnet-outdated/dotnet-outdated](https://github.com/dotnet-outdated/dotnet-outdated)

Pull requests welcome!



@martin_costello



@martincostello



These
slides



Thank you! 🧑

@martin_costello



@martincostello

