

ELECTRON

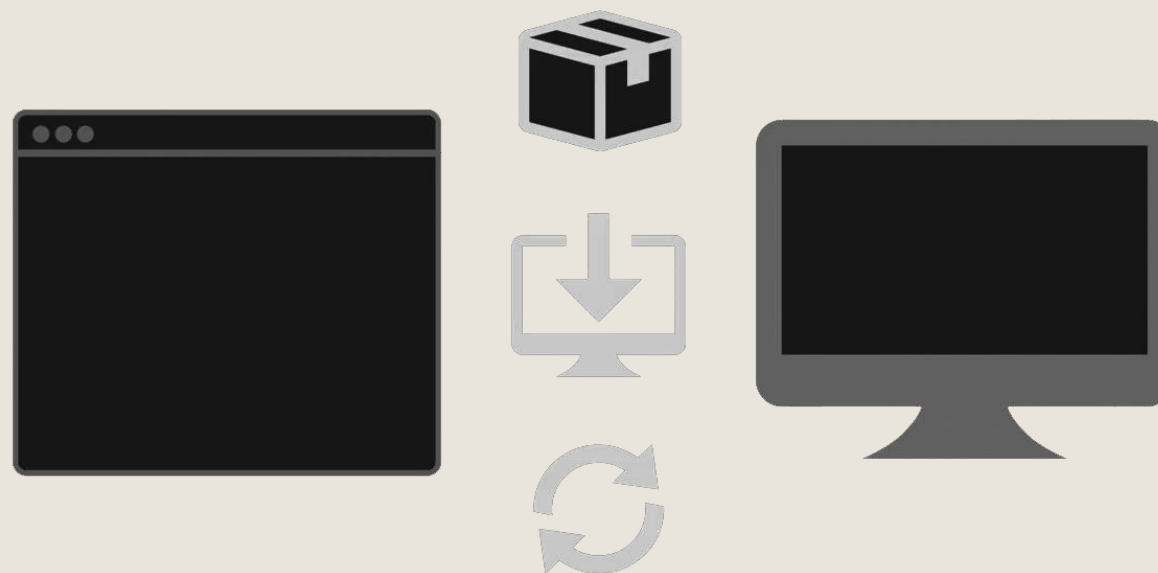
André Oliveira, nº44598



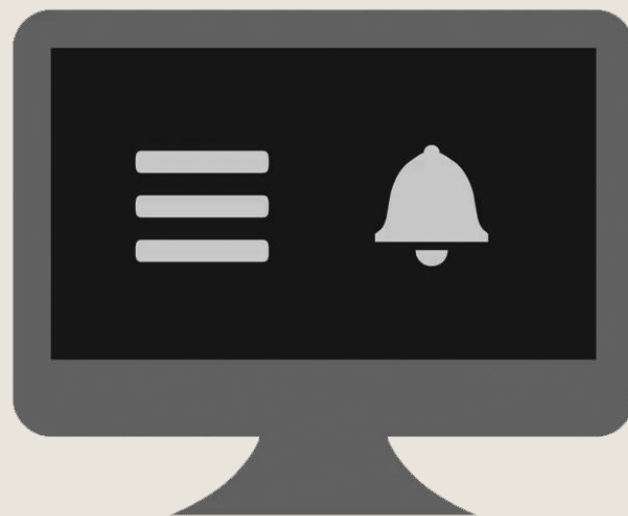
Agenda

- Introdução
- Electron
 - *O que é?*
 - *Como funciona?*
- Considerações
- Aplicações

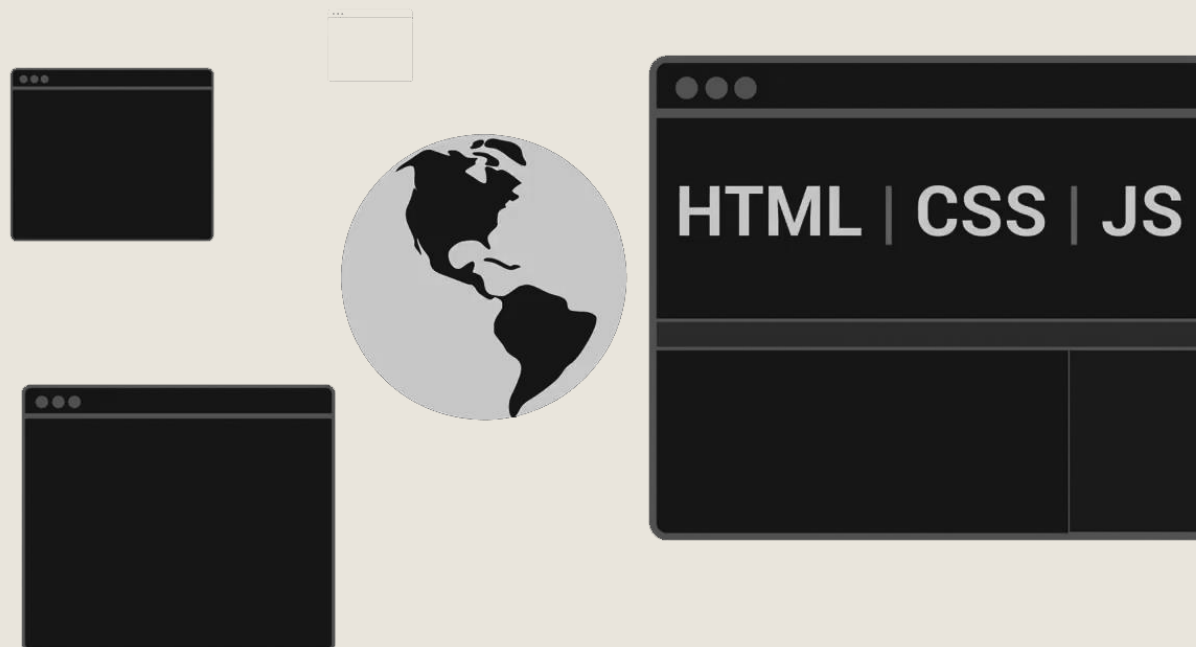
Aplicações *Desktop*



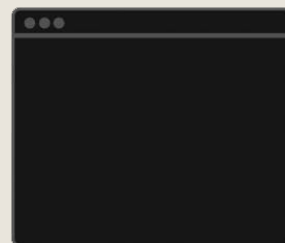
Aplicações *Desktop*



Aplicações *Web*



Aplicações *Web*



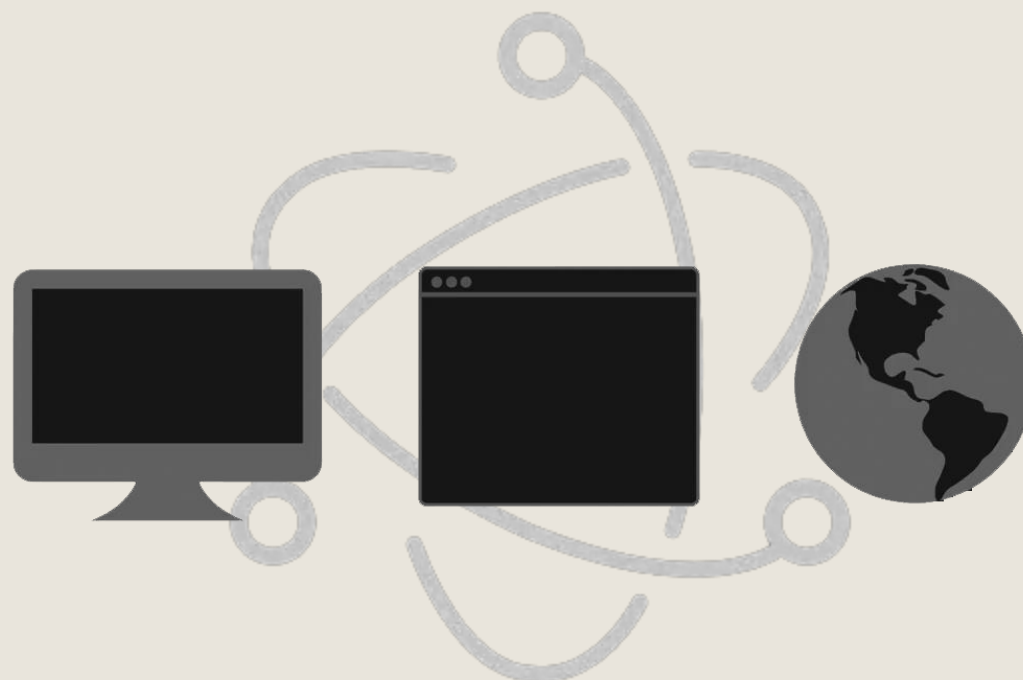
Introdução

Electron

Considerações

Aplicações

ELECTRON



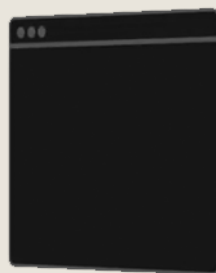
O que é?

É uma *framework open-source* desenvolvida pelo GitHub para criar aplicações multiplataforma utilizando HTML, CSS e JavaScript.



Através da combinação do Chromium e Node.js permite empacotar as aplicações para Mac, Windows e Linux.

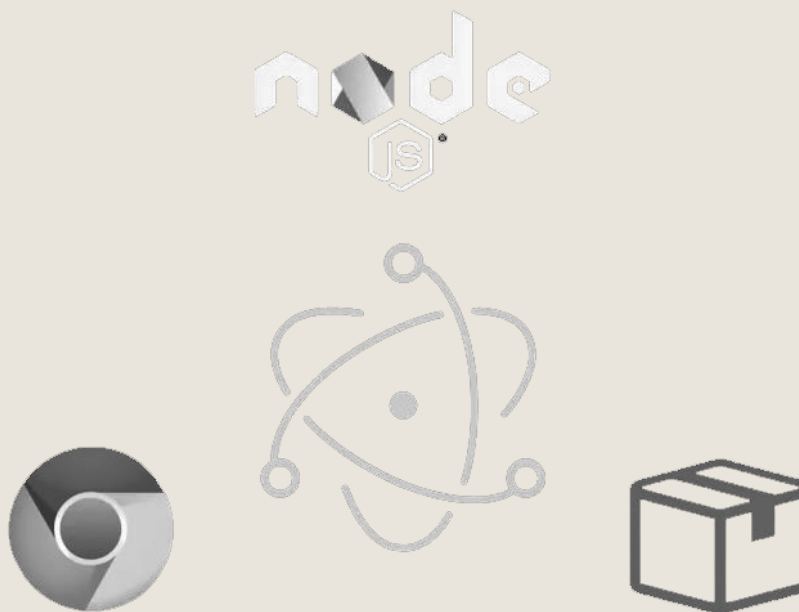
Particularidades



Particularidades

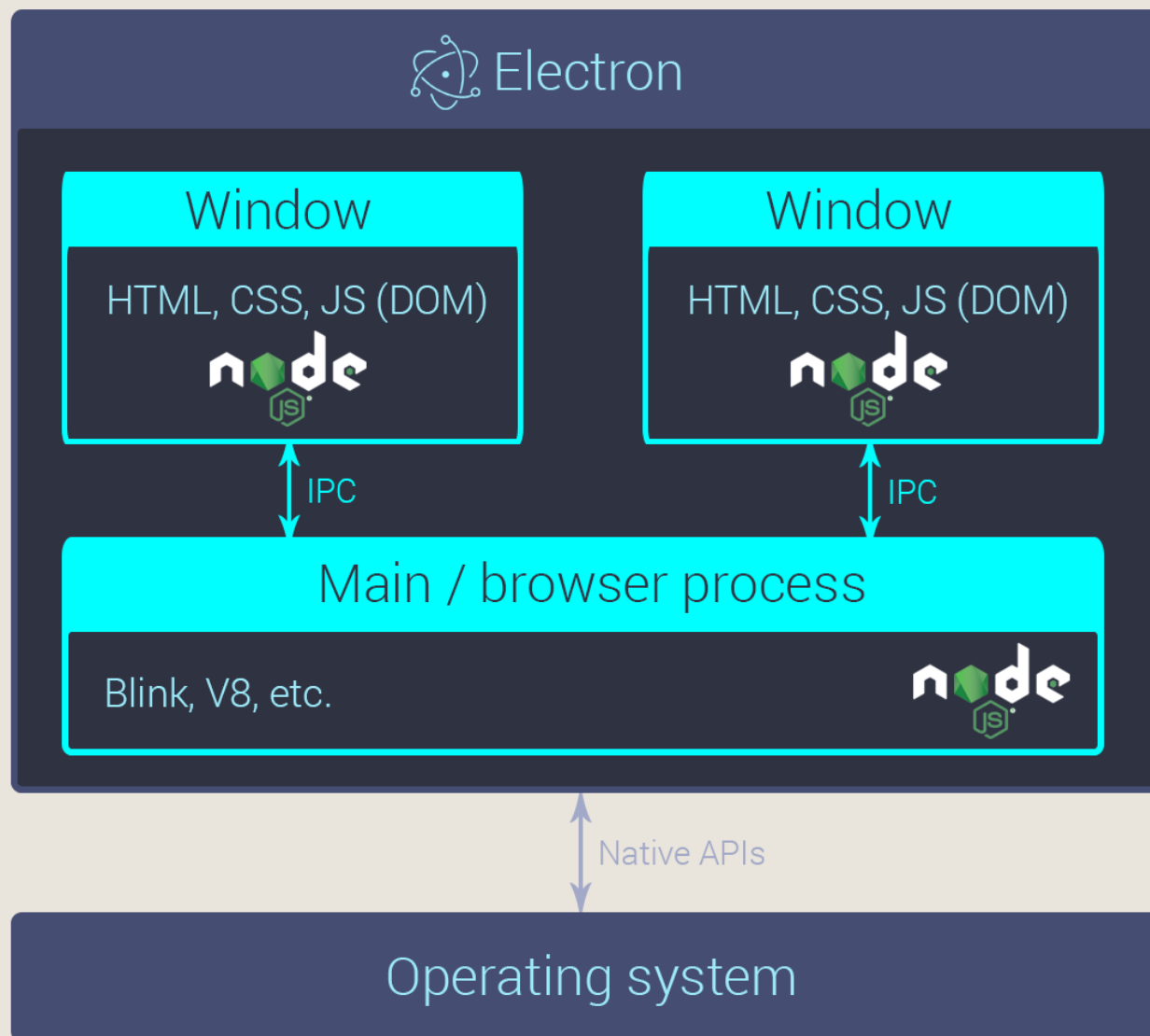


Particularidades



Como funciona?

- À semelhança de uma aplicação web existe um *script package.json* que é considerado como o **Processo Main** – *só existe um único*
- O *scrip* que corre o **Main** pode gerar um GUI através de criação de páginas web, e é responsável pela gestão da interação do GUI nativo do sistema operativo.
- As páginas web são criadas com o Chromium, e desta forma partilham a mesma arquitetura de multi-processo, ou seja, cada página tem o seu próprio **Processo de Renderização**.
- O **Processo de Renderização** utiliza um ficheiro HTML que referênciia os ficheiros comuns de CSS, JavaScript, imagens, etc. e renderiza-o numa janela.
- Em browser normais, as páginas web geralmente correm num ambiente contido e não são autorizadas a aceder aos recursos nativos. Porém como o **Electron** utiliza a API do Node.js nas páginas web, tem a capacidade de executar operações de mais baixo nível.





Vantagens


- Multiplataforma
 - Baixos custos de desenvolvimento
 - HTML, CSS, JS
 - Aplicações ***Electron*** são semelhantes a aplicações web
 - Atualizações automáticas
- *Todas estas vantagens possibilitam a abstração de vários problemas, permitindo que todos os **recursos** sejam focados apenas no desenvolvimento da solução que se pretende implementar.*

Desvantagens


- “Overhead”
- Segurança
- Proteção do código

 Common Vulnerabilities and Exposures	
HOME > CVE > CVE-2018-1000136	
CVE-ID	
CVE-2018-1000136	Learn more at National Vulnerability Database • CVSS Severity Rating • Fix Information • Vulnerable Software
Description	Electron version 1.7 up to 1.7.12; 1.8 up to 1.8.3 and 2.0.0 up to 2.0.0-beta.3 contains a vulnerability that allows execution of 3rd party code AND disallows node integration AND has not specified if webview is enabled.
References	Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities.
	<ul style="list-style-type: none">MISC:https://www.electronjs.org/blog/webview-fixMISC:https://www.trustwave.com/Resources/SpiderLabs-Blog/CVE-2018-1000136--
Assigning CNA	
MITRE Corporation	
Date Entry Created	
20180321	Disclaimer: The entry creation date may reflect when the entry was created or updated in CVE.

 ELECTRON

Donors Apps Docs Blog Community Governance Releases Search  English

Webview Vulnerability Fix

March 21, 2018  ckerr

A vulnerability has been discovered which allows Node.js integration to be re-enabled in some Electron applications that disable it. This vulnerability has been assigned the CVE identifier [CVE-2018-1000136](#).

Affected Applications

An application is affected if *all* of the following are true:

1. Runs on Electron 1.7, 1.8, or a 2.0.0-beta
2. Allows execution of arbitrary remote code
3. Disables Node.js integration
4. Does not explicitly declare `webviewTag: false` in its webPreferences
5. Does not enable the `nativeWindowOption` option
6. Does not intercept `new-window` events and manually override `event.newGuest` without using the supplied `newGuest` function

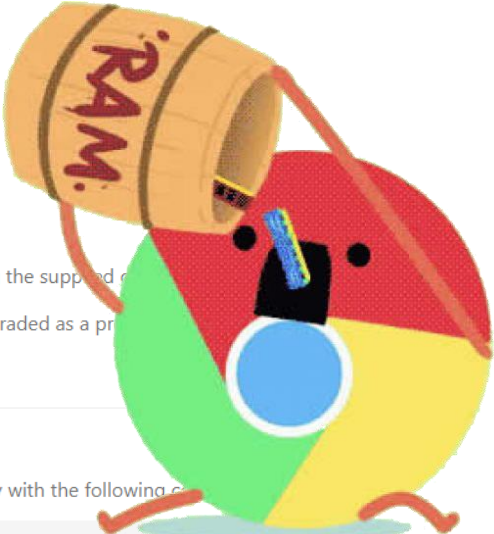
Although this appears to be a minority of Electron applications, we encourage all applications to be upgraded as a precaution.

Mitigation

This vulnerability is fixed in today's [1.7.13](#), [1.8.4](#), and [2.0.0-beta.5](#) releases.

Developers who are unable to upgrade their application's Electron version can mitigate the vulnerability with the following code:

```
app.on('web-contents-created', (event, win) => {
  win.on('new-window', (event, newURL, frameName, disposition,
```



Introdução

Electron

Considerações

Aplicações

Aplicações *desktop* construídas com *Electron*



DISCORD



slack



Visual Studio Code



ATLASSIAN

Questões

