Menos Gandalfs e mais John Wicks

Menos frameworks mágicos e mais engenharia de software

@chengjunior

TEMPEST
Protegendo negócios no mundo digital

Já usou uma dessas mágicas?

- Struts
- Spring boot
- JSF
- Rails
- Django
- GORM
- Laravel
- Symfony
- Node.js
- Golang
- ...







Do início





A magia acabou!

Início da saga pelo feiticeiro no Go

Vou fazer minha magia

Magia deu errado

Fazer o básico com transparência

O John Wick nasce

E a segurança?

Poder no código

Feitiçarias pesadas


0-day

Feitiço fail


Acabei!!

Surge das cinzas

Mestre dos magos


E agora?

Historinha do Carnaval

Vulnerability Details : CVE-2013-0277

ActiveRecord in Ruby on Rails before 2.3.17 and 3.x before 3.1.0 allows remote attackers to cause a denial of service or execute arbitrary code via crafted serialized attributes that cause the +serialize+ helper to deserialize arbitrary YAML.

Publish Date : 2013-02-12 Last Update Date : 2019-08-08

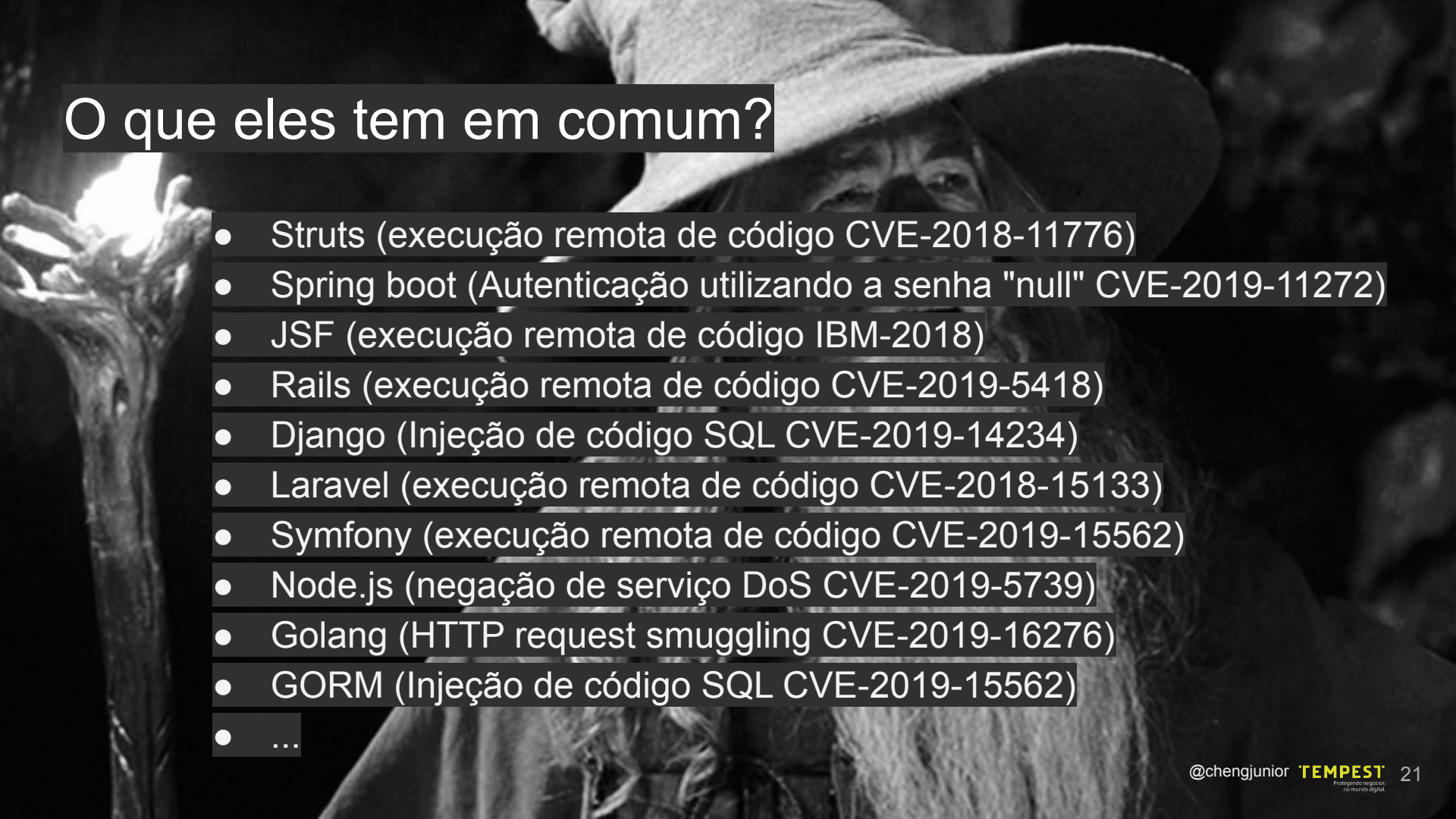
Collapse All Expand All Select Select&Copy Scroll To Comments External Links

Search Twitter Search YouTube Search Google

− CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service Execute Code
CWE ID	CWE id is not defined for this vulnerability


ON RAILS

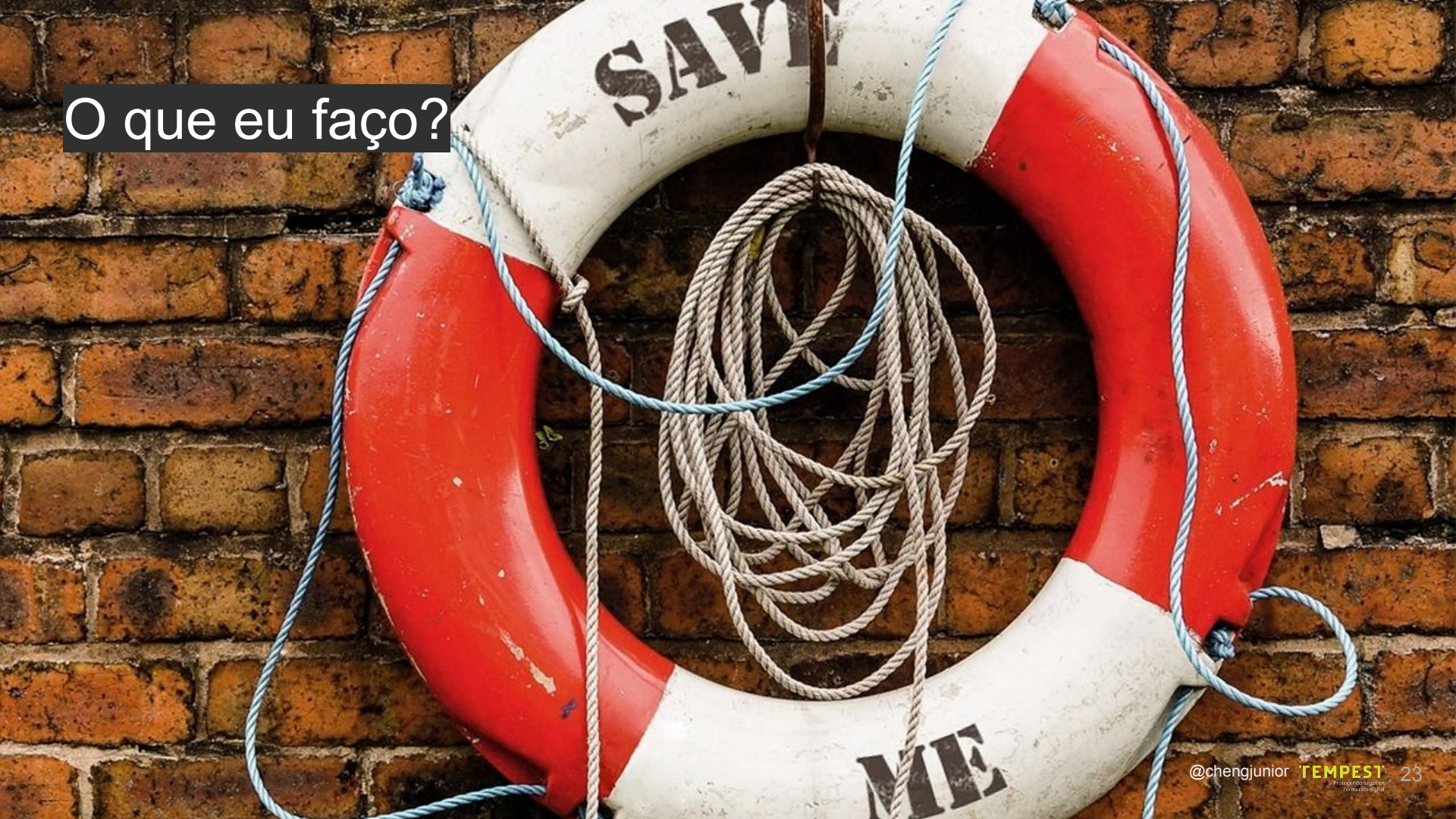


O que eles tem em comum?

- Struts (execução remota de código CVE-2018-11776)
- Spring boot (Autenticação utilizando a senha "null" CVE-2019-11272)
- JSF (execução remota de código IBM-2018)
- Rails (execução remota de código CVE-2019-5418)
- Django (Injeção de código SQL CVE-2019-14234)
- Laravel (execução remota de código CVE-2018-15133)
- Symfony (execução remota de código CVE-2019-15562)
- Node.js (negação de serviço DoS CVE-2019-5739)
- Golang (HTTP request smuggling CVE-2019-16276)
- GORM (Injeção de código SQL CVE-2019-15562)
- ...

Reinventar a roda?

O que eu faço?



Ser John Wick

@chengjunior