SBSI2018
XIV SIMPÓSIO BRASILEIRO DE SISTEMAS DE INFORMAÇÃO
4 A 8 DE JUNHO - CAMPUS-SEDE - CAXIAS DO SUL/RS
SBC Sociedade Brasileira de Computação

Improvements to the Identification Process of Known Vulnerable Components: Deciding About Updates

Bruna Mocelin; Kleinner Farias; Lucian Gonçales; Vinicius Bischoff

Programa de Pós Graduação em Computação Aplicada (PPGCA)

Universidade do Vale do Rio dos Sinos (UNISINOS)

Visão Geral

- Vulnerabilidades
- Componentes Vulneráveis Conhecidos
- Dep|ct
- Método de avaliação
- Resultados
- Considerações Finais
- Trabalhos Futuros

Vulnerabilidades

"A weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability." (Dicionário da CVE)

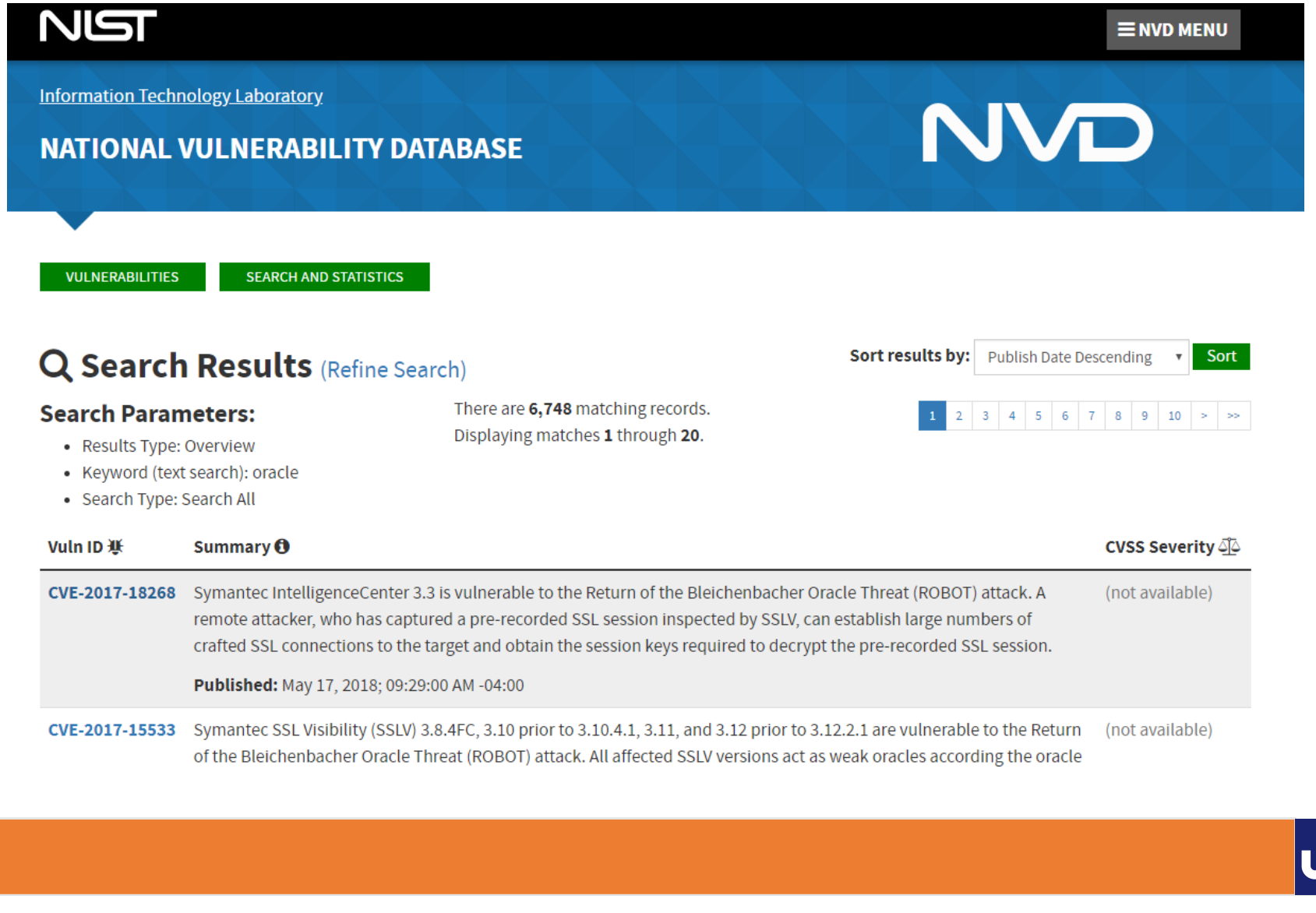
Vulnerabilidades

- Originados de:
  - Más práticas de implementação;
  - Fragilidade nos processos internos do sistema;
  - Falhas no controle de segurança;
  - Utilização de componentes com vulnerabilidades já identificadas...

Componentes Vulneráveis Conhecidos

- Componentes que contém vulnerabilidades catalogadas em uma base de dados ou dicionários:
  - *National Vulnerabilities Database* (NVD);
  - *Common Vulnerabilities and Exposures (CVE).*

Componentes Vulneráveis Conhecidos



Componentes Vulneráveis Conhecidos

Common Vulnerabilities and Exposures

CVE List CNAs Board About News & Blog

NVD
Go to for:
CVSS Scores
CPE Info
Advanced Search

Search CVE List | Download CVE | Data Feeds | Request CVE IDs | Update a CVE Entry

TOTAL CVE Entries: 101528

HOME > CVE > SEARCH RESULTS

Search Results

There are **1772** CVE entries that match your search.

Name	Description
CVE-2018-8119	A spoofing vulnerability exists when the Azure IoT Device Provisioning AMQP Transport library improperly validates certificates over the AMQP protocol, aka "Azure IoT SDK Spoofing Vulnerability." This affects C# SDK, C SDK, Java SDK.
CVE-2018-8015	In Apache ORC 1.0.0 to 1.4.3 a malformed ORC file can trigger an endlessly recursive function call in the C++ or Java parser. The impact of this bug is most likely denial-of-service against software that uses the ORC file parser. With the C++ parser, the stack overflow might possibly corrupt the stack.
CVE-2018-7739	antsle antman before 0.9.1a allows remote attackers to bypass authentication via invalid characters in the username and password parameters, as demonstrated by a username=>&password=%0a string to the /login URI. This allows obtaining root permissions within the web management console, because the login process uses Java's ProcessBuilder class and a bash script called antsle-auth with insufficient input validation.
CVE-2018-5487	NetApp OnCommand Unified Manager for Linux versions 7.2 through 7.3 ship with the Java Management Extension Remote Method Invocation (JMX RMI) service bound to the network, and are susceptible to unauthenticated remote code execution.
CVE-2018-5486	NetApp OnCommand Unified Manager for Linux versions 7.2 though 7.3 ship with the Java Debug Wire Protocol (JDWP) enabled which allows unauthorized local attackers to execute arbitrary code.
CVE-2018-2841	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2 and 12.2.0.1. Difficult to exploit vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via multiple protocols to compromise Java VM. While the vulnerability is in Java VM, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java VM. CVSS 3.0 Base Score 8.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).

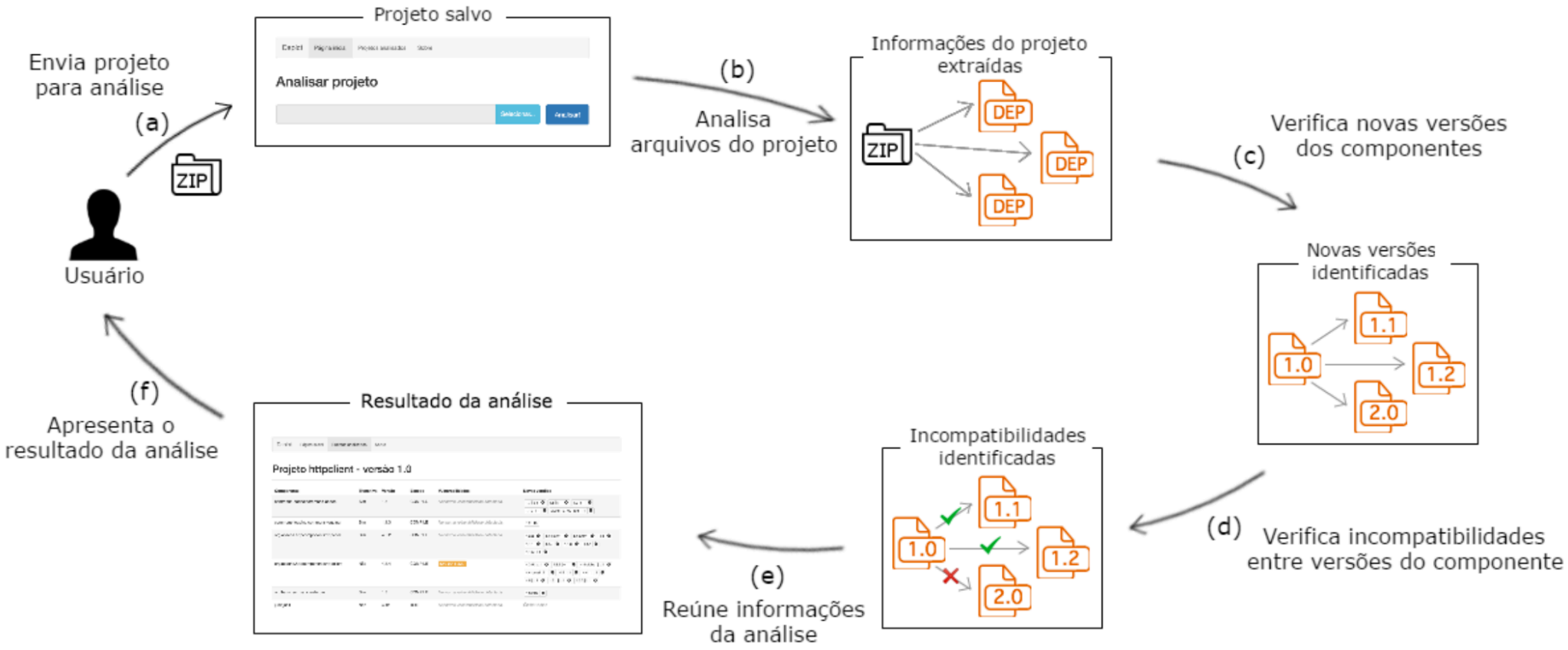
Componentes Vulneráveis Conhecidos

- *Como tratar e gerenciar componentes com vulnerabilidades?*
  - *Utilizar ferramentas para gerenciar componentes vulneráveis conhecidos;*
    - *Contém uma série de problemas que ainda assim dificultam análise e suporte a atualização de componentes com vulnerabilidades conhecidas…*

Componentes Vulneráveis Conhecidos

- **RF01**: utilizar e manter fontes de dados atualizadas.
- **RF02**: integração de fontes de dados distintas de vulnerabilidades;
- **RF03**: permitir extração de dependências de diferentes tipos de projetos;
- **RF04**: listar novas versões do componente;
- **RF05**: listar incompatibilidades entre a versão atual e a nova versão do componente;
- **RF06**: identificar propagação de atualizações;
- **RF07**: listar vulnerabilidades das outras versões do componente;
- **RNF1**: possibilidade de integrar a ferramenta no processo de desenvolvimento de software.

DEP|CT


Envia projeto para análise
(a)
ZIP
Usuário
Projeto salvo
Analisar projeto
(b)
Analisa arquivos do projeto
Informações do projeto extraídas
ZIP
DEP
DEP
DEP
(c)
Verifica novas versões dos componentes
Novas versões identificadas
1.0
1.1
1.2
2.0
(d)
Verifica incompatibilidades entre versões do componente
Incompatibilidades identificadas
1.0
1.1
1.2
2.0
(e)
Reúne informações da análise
Resultado da análise
Projeto httpclient - versão 1.0
(f)
Apresenta o resultado da análise

DEP|CT

dep|ct Página inicial Projetos analisados Sobre

Projeto exemplo - versão 1.0

Há novas versões disponíveis para as dependências deste projeto.
Novas versões sugeridas:
org.apache.httpcomponents:httpclient:4.5.2 4

Componente	▲Transitiva	Versão	Escopo	Vulnerabilidades	Novas versões
org.apache.httpcomponents:httpclient	Não	4.3.4	COMPILE	CVE-2014-3577 1	4.3.5 | v: 1 · 4.3.6 3 · 4.4 | i: 2 2 · 4.4.1 | i: 2 · 4.5 | i: 2 · 4.5.1 | i: 2 · 4.5.2 | i: 2
junit:junit	Não	4.12	TEST	*Nenhuma vulnerabilidade detectada.*	*Última versão*
org.apache.httpcomponents:httpcore	Sim	4.3.2	COMPILE	*Nenhuma vulnerabilidade detectada.*	4.3.3 · 4.4 · 4.4.1 · 4.4.2 · 4.4.3 · 4.4.4 · 4.4.5 | i: 4
commons-logging:commons-logging	Sim	1.1.3	COMPILE	*Nenhuma vulnerabilidade detectada.*	1.2
commons-codec:commons-codec	Sim	1.6	COMPILE	*Nenhuma vulnerabilidade detectada.*	1.7 | i: 8 · 1.8 | i: 8 · 1.9 | i: 8 · 1.10 | i: 8
org.hamcrest:hamcrest-core	Sim	1.3	TEST	*Nenhuma vulnerabilidade detectada.*	*Última versão*

UNISINOS

Método de Avaliação

Descrição dos projetos selecionados

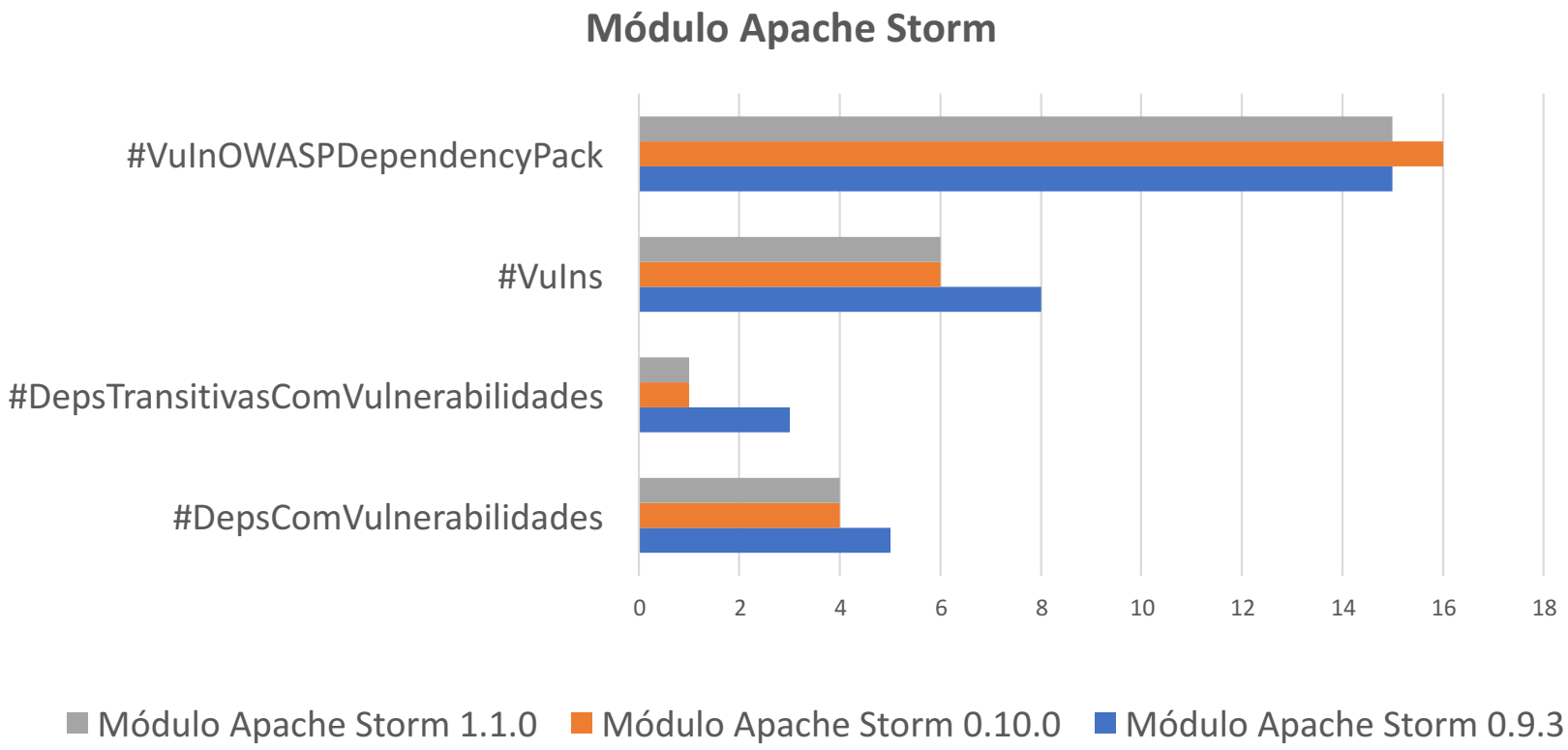
Característica	Apache Storm	Activiti
Descrição	Sistema de computação distribuído que permite processar dados em tempo real.	Plataforma de gerenciamento de processos de negócio (BPM) e fluxo de trabalho.
Módulo	Storm-core	Activiti-engine
Website	http://storm.apache.org/	http://activiti.org/
Repositório	https://github.com/apache/storm	https://github.com/Activiti/Activiti
Versões Selecionadas	0.9.3 (19/11/2014) 0.10.0 (23/10/2015) 1.1.0 (15/07/2016)	5.0 (31/01/2011) 5.14 (21/10/2013) 5.21.0 (13/06/2016)

Método de Avaliação

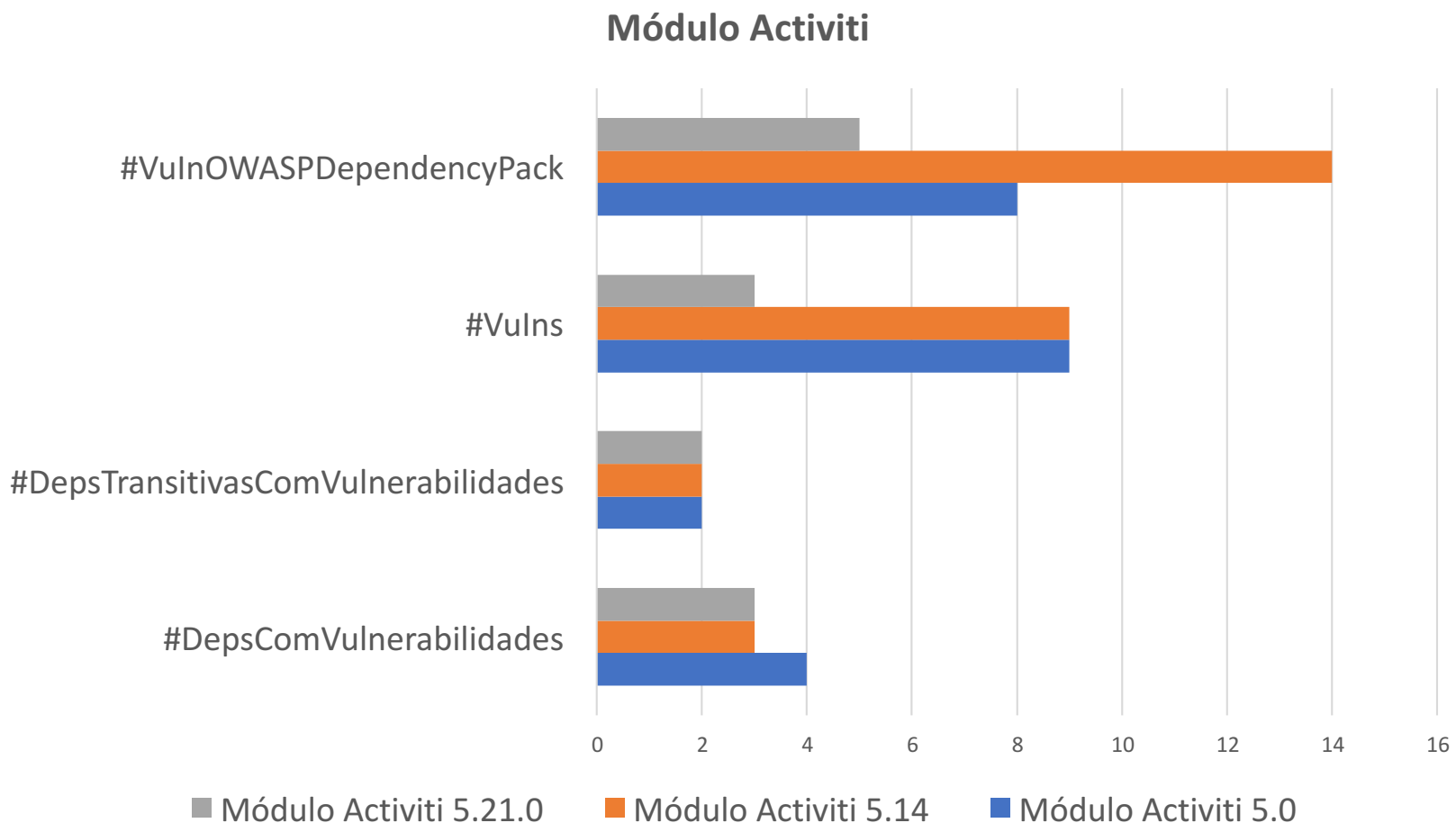
Descrição das Métricas analisadas.

Métrica	Descrição
#VulnsOWASPDependencyCheck	# total de vulnerabilidades detectadas pela ferramenta OWASP *Dependency Check*
#Vulns	# total de vulnerabilidades detectadas
#DepsTransitivasComVulnerabilidades	# dependências transitivas com vulnerabilidades.
#DepsComVulnerabilidades	# total de dependências com vulnerabilidades.

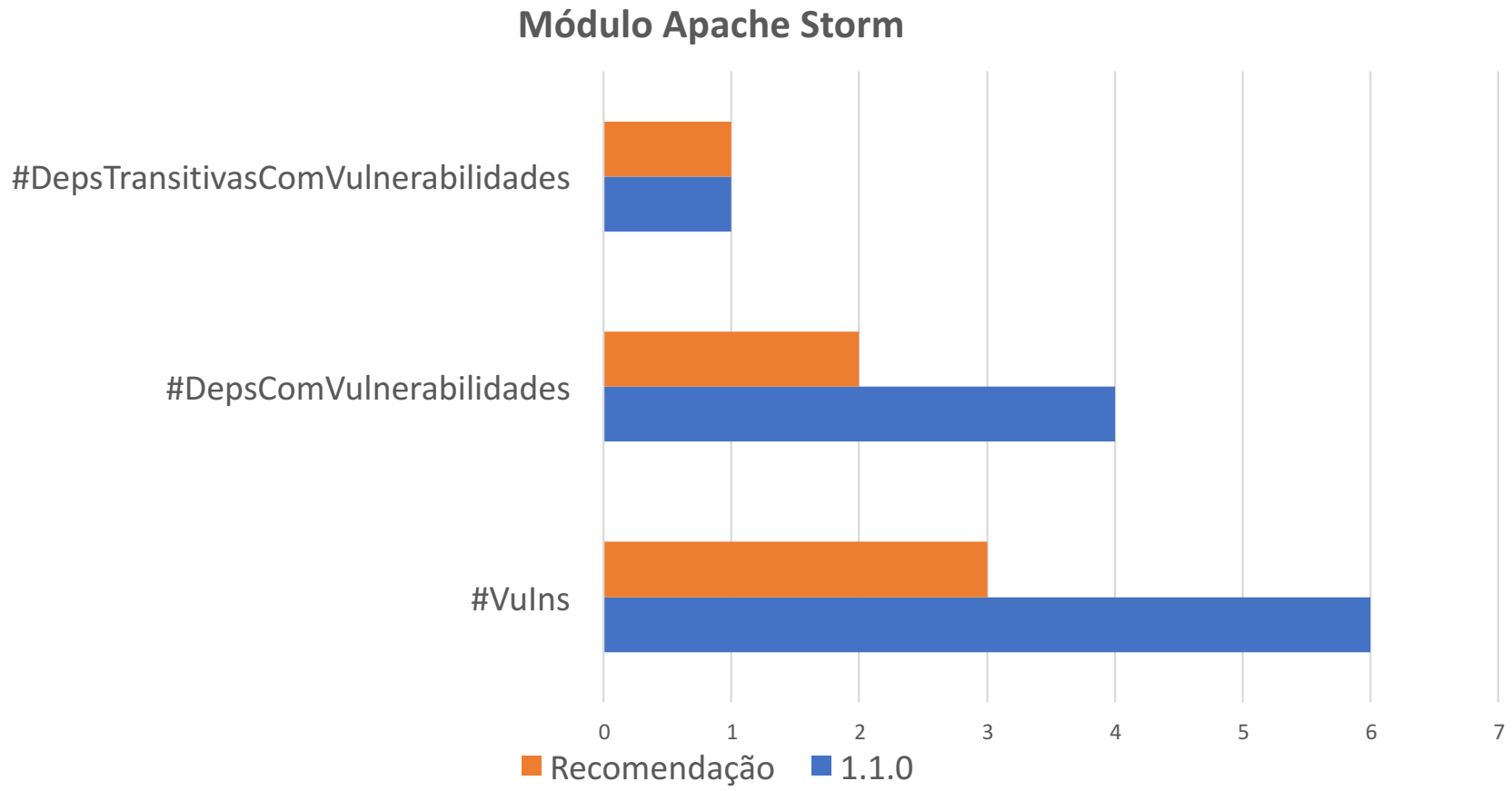
Resultados


Módulo Apache Storm
#VuInOWASPDependencyPack
#VuIns
#DepsTransitivasComVulnerabilidades
#DepsComVulnerabilidades
0
2
4
6
8
10
12
14
16
18
Módulo Apache Storm 1.1.0
Módulo Apache Storm 0.10.0
Módulo Apache Storm 0.9.3

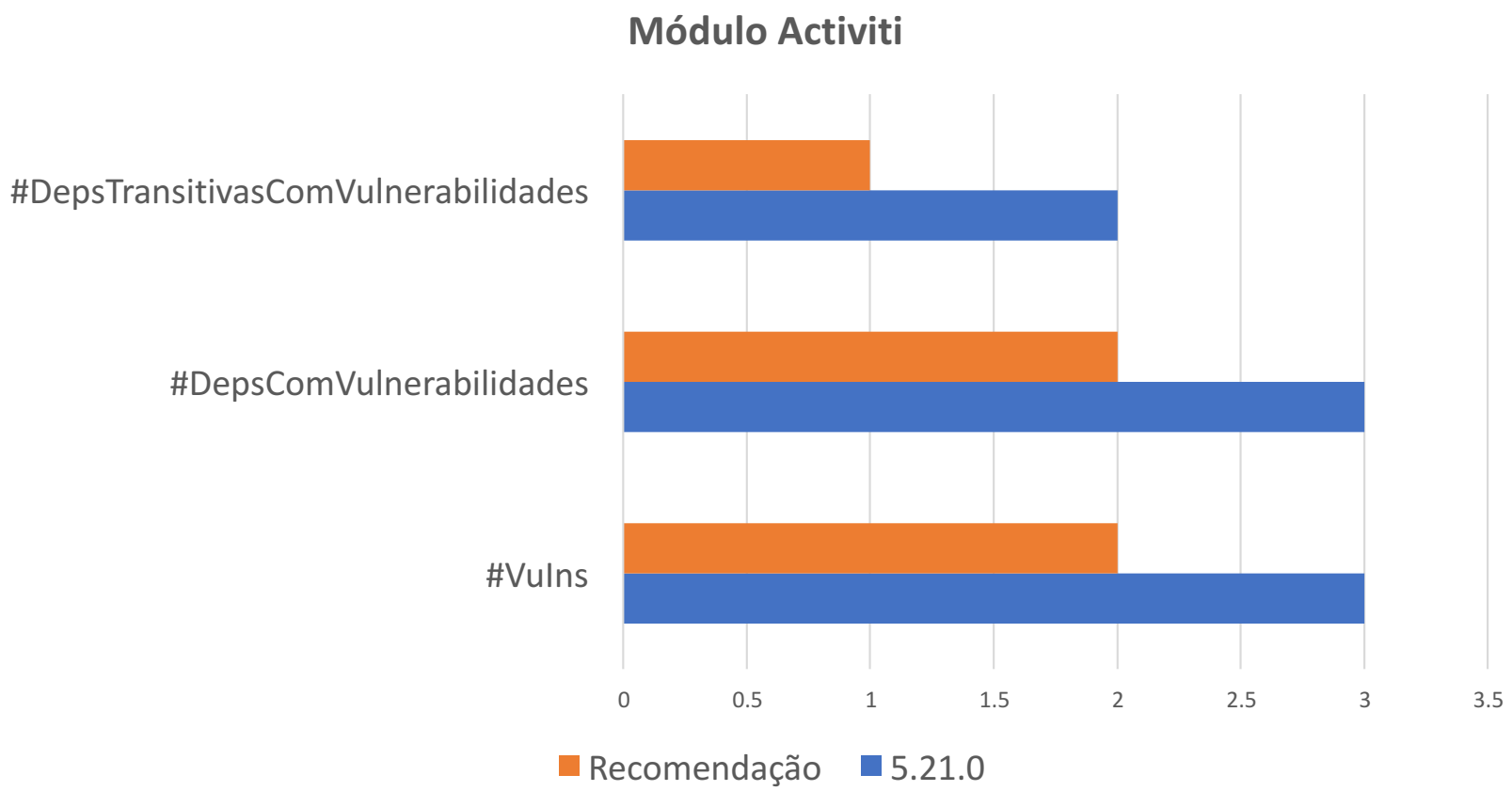
Resultados


Módulo Activiti
#VuInOWASPDependencyPack
#VuIns
#DepsTransitivasComVulnerabilidades
#DepsComVulnerabilidades
0
2
4
6
8
10
12
14
16
Módulo Activiti 5.21.0
Módulo Activiti 5.14
Módulo Activiti 5.0

Resultados


Módulo Apache Storm
#DepsTransitivasComVulnerabilidades
#DepsComVulnerabilidades
#VulIns
0
1
2
3
4
5
6
7
Recomendação
1.1.0

Resultados


Módulo Activiti
#DepsTransitivasComVulnerabilidades
#DepsComVulnerabilidades
#Vulns
0
0.5
1
1.5
2
2.5
3
3.5
Recomendação
5.21.0

Considerações Finais

- Gerenciar componentes vulneráveis conhecidos é um problema relevante;
- Falta de suporte a decisão de atualizações;
  - Neste contexto foi proposto a DEP|CT;
- Resultados demonstram que a ferramenta pode ser utilizada para:
  - Analisar e mitigar os componentes vulneráveis conhecidos;
  - Decidir sobre a aplicação da atualização;

Trabalhos Futuros

- Aprimorar a associação entre vulnerabilidades e dependências;
- Permitir integração com sistemas de controle de versão;
- Implementar sistemas de notificações em tempo real.

Referências

[1] Allen, Julia. Why is Security a Software Issue?. EDPACS: The EDP Audit, Control, and Security Newsletter, Pittsburgh, v. 36, n. 1, (Aug. 2007) p. 1-13. Disponível em: <http://www.tandfonline.com/doi/ref/10.1080/07366980701500734>. Acesso em: 13 fev. 2018.

[2] Farias, K., Garcia, A., Whittle, J., Chavez, C. V. F. G., & Lucena, C. (2015). Evaluating the effort of composing design models: a controlled experiment. *Software & Systems Modeling*, *14*(4), 1349-1365.

[3] Alqahtani, S. S., Eghan, E. E., & Rilling, J. Tracing known security vulnerabilities in software repositories–A Semantic Web enabled modeling approach. *Science of Computer Programming*, *121*, 2016, 153-175.

[4] Cadariu, M. Tracking Known Security Vulnerabilities in Third-party Components, Netherlands. 2014. 86 f. M. Sc. Dissertation - Programa de Pós-Graduação em Ciência da Computação, Delft University of Technology, Holanda, 2014.

[5] Cadariu, M.; Bowers, E.; Visser, J.; Deuresen, A. V. Tracking Known Security Vulnerabilities in Proprietary Software Systems. In: 2015 *IEEE 22nd International Conference on Software Analysis, Evolution, and Reengineering,* (Montreal, QC, Março 2015), SANER, 516-519.

[6] Cheikes, B. A.; Waltermire, D.; Scarfone, K. Common Platform Enumeration: Naming Specification Version 2.3. National Institute of Standards and Technology (NIST), Gaithersburg, Aug. 2011.

[7] Durumeric, Zakir et al. The Matter of Heartbleed. *Proceedings of the 2014 Conference on Internet Measurement Conference*, (Vancouver, Quebec, Nov. 2014), 475-488.

[8] Financial Services Information Sharing and Analysis Center. Appropriate Software Security Control Types for Third Party Service and Product Providers., Oct. 2015.

[9] Fonseca, V. S.; Barcellos; M. P; Almeida Falbo, R. Tools Integration for Supporting Software Measurement: A Systematic Literature Review. *iSys-Revista Brasileira de Sistemas de Informação*, *8*,4, 2016, 80-108.

[10] Gosling, J.; Joy, B.; Steele, G.; Bracha, G.; Buckley, A. The Java Language Specification: Java SE 8 Edition. Redwood City: Oracle America, Inc. and/or its affiliates, 2015. Disponível em: <http://docs.oracle.com/javase/ specs/jls/se8/jls8.pdf>. Acesso em: 10 jan. 2018.

[11] Mcgraw, G. Software Security: Building Security In. Upper Saddle River, NJ: Addison-Wesley, 2006.

[12] Plate, H.; Ponta, S. E.; Sabetta, A. Impact Assessment for Vulnerabilities in Open-source Software Libraries. In: *2015 IEEE International Conference on Software Maintenance and Evolution.* (Bremen, Sept. 2015), (ICSME), 411-420.

[13] Whitesource Software. Continuously Audit Open Source Components in Your Code. New York, 2016. Disponível em: <http://www.whitesourcesoftware.com /open_source_scann ing_software/>. Acesso em: 20 fev. 2018 .

Contato:

Lucian Gonçales

lucianjosegoncales@gmail.com