Universidade do Minho
Mestrado Integrado em Engenharia Informática
Tecnologia de Segurança
TP1 - Parte A
Vulnerabilidades e Exposições Comuns (CVE)

1 - Objectivos:

Este trabalho prático tem por objectivo principal apresentar a identificação padrão de vulnerabilidades e exposições publicamente conhecidas, assim como a sua importância nas atividades relacionadas com a segurança de sistemas informáticos. Espera-se, com este trabalho, promover o conhecimento de ferramentas de apoio a ações proativas de segurança.

2 - CVE - Common Vulnerabilities and Exposures

As vulnerabilidades e exposições comuns (CVEs) consistem em uma lista de nomes padronizados para vulnerabilidades e outras informações relacionadas com exposições à segurança conhecidas publicamente. O seu objetivo de padronização facilita a distribuição de informações em diferentes bancos de dados de vulnerabilidades e ferramentas de segurança, tornando a sua busca mais simples e uniforme. É importante ressaltar que o CVE não é, por si, um banco de dados de vulnerabilidades, mas um sistema de identificação destas.

A CVE é mantida pela MITRE Corporation e é também responsável pela moderação do Editorial Board, composto por representantes de organizações relacionadas com segurança de sistemas, como instituições académicas, orgãos governamentais, iniciativa privada, além de especialistas em segurança. A atribuição de identificadores é feita por CVE Numbering Authorities (CNA) e seguem a sintaxe detalhada em https://cve.mitre.org/cve/identifiers/syntaxchange.html#new, onde também é possível identificar todos os CNAs.

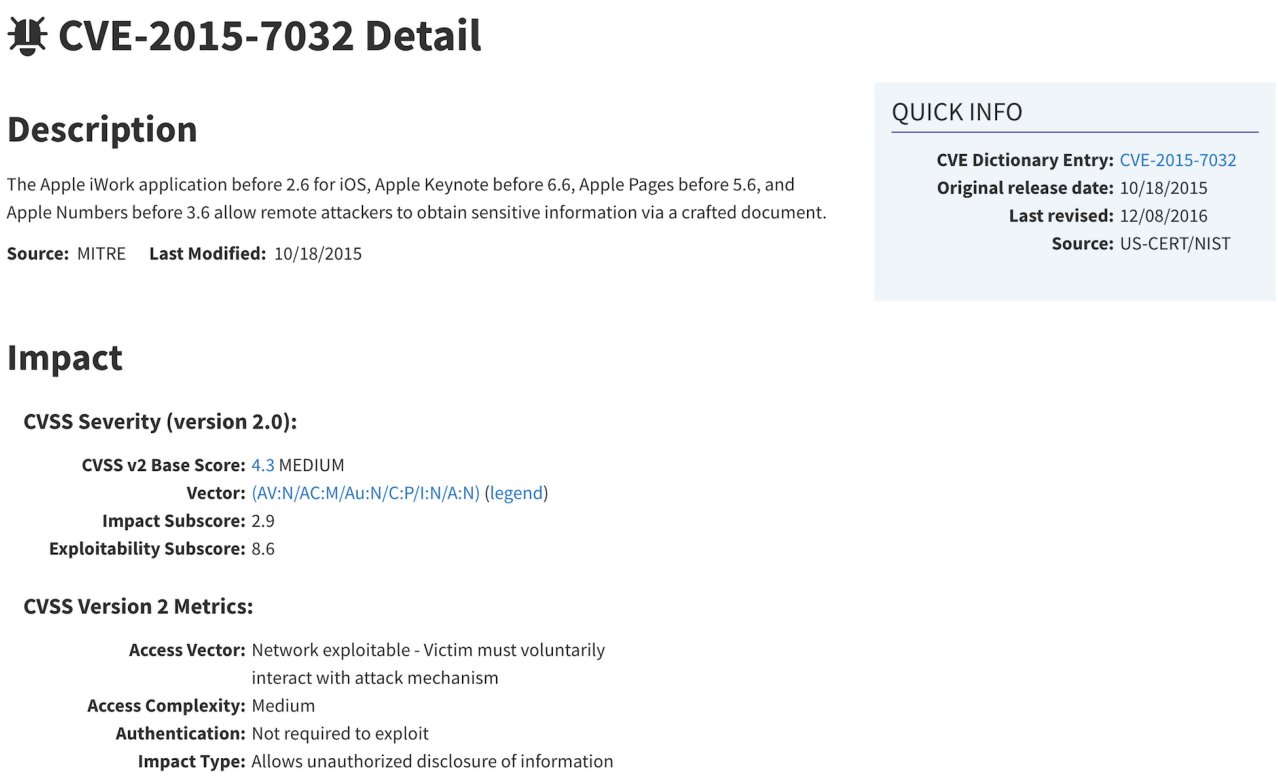
As informações sobre CVEs, assim como a lista completa podem ser encontrados em https://cve.mitre.org/. Um exemplo de identificador CVE é apresentado na figura abaixo.

CVE-ID	
CVE-2015-7032	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
The Apple iWork application before 2.6 for iOS, Apple Keynote before 6.6, Apple Pages before 5.6, and Apple Numbers before 3.6 allow remote attackers to obtain sensitive information via a crafted document.	

3 - Bases de dados de Vulnerabilidades

As bases de dados de vulnerabilidade são responsáveis por manter informações detalhadas sobre vulnerabilidades conhecidas e identificadas via CVEs. Isto inclui a gravidade da vulnerabilidade, versões afetadas, correções liberadas, entre outros. Uma das principais bases de dados pública é *National Vulnerability Database* - NVE (https://nvd.nist.gov/), mantida pelo governo americano.

Tomando como exemplo a vulnerabilidade apresentada na figura da Secção 2, as informações detalhadas na base NVE é apresentada na Figura abaixo.



CVE-2015-7032 Detail

Description

The Apple iWork application before 2.6 for iOS, Apple Keynote before 6.6, Apple Pages before 5.6, and Apple Numbers before 3.6 allow remote attackers to obtain sensitive information via a crafted document.

Source: MITRE **Last Modified:** 10/18/2015

QUICK INFO

CVE Dictionary Entry: CVE-2015-7032
Original release date: 10/18/2015
Last revised: 12/08/2016
Source: US-CERT/NIST

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 4.3 MEDIUM
Vector: (AV:N/AC:M/Au:N/C:P/I:N/A:N) (legend)
Impact Subscore: 2.9
Exploitability Subscore: 8.6

CVSS Version 2 Metrics:

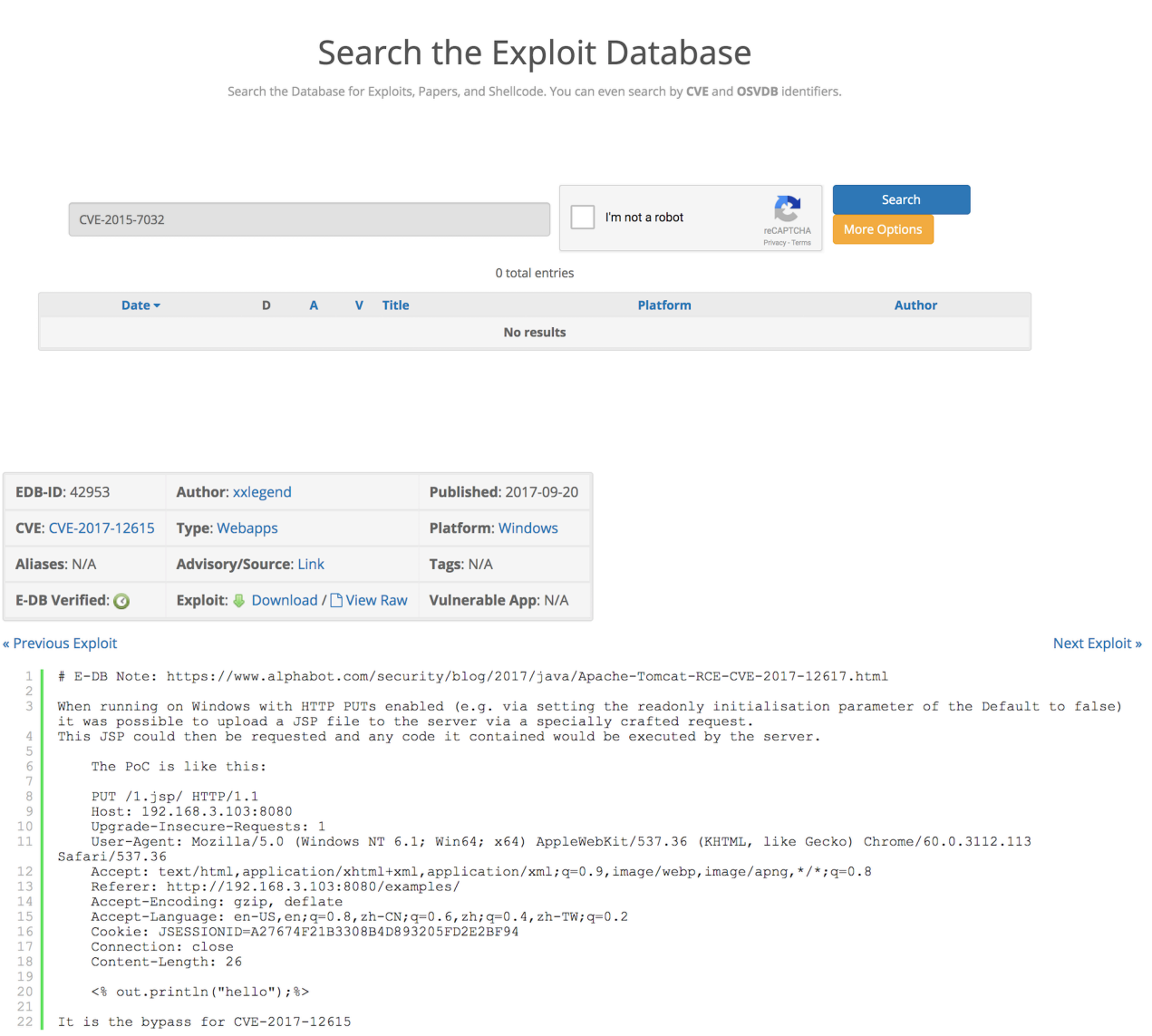
Access Vector: Network exploitable - Victim must voluntarily interact with attack mechanism
Access Complexity: Medium
Authentication: Not required to exploit
Impact Type: Allows unauthorized disclosure of information

Analise a figura e tente identificar as informações detalhadas nela apresentadas.

4 - Bases de dados de explorações

A existência de uma vulnerabilidade conhecida não implica a existência de meios conhecidos sobre como explorá-las. Neste sentido, algumas bases de dados mantêm informações sobre os mecanismos de exploração conhecidos para uma vulnerabilidade identificada via CVE. A mais conhecida delas é a Exploit-db (https://www.exploit-db.com/). Estas tendem a ser informações mais sensíveis e exigem cuidado e autorização expressa para testes em uma infraestrutura em funcionamento.

Como pode ser observado nas figuras abaixo, a vulnerabilidade identificada nas aplicações de escritório Apple via CVE-2015-7032 não possuía, na data da consulta, uma forma de exploração identificada na exploit-db. Contudo, a vulnerabilidade recentemente identificada no Apache Tomcat versão 9.0.1 ou inferior, com CVE-2017-12615, possui um *exploit* listado nesta base de dados.



5 - Exercícios

5.1 - Escolha três aplicações tipicamente usadas em seu computador pessoal, pesquise pela existência de vulnerabilidades conhecidas e meios de explorá-las. Descreva detalhadamente as suas descobertas, incluindo as imagens de suas pesquisas e a descrição das informações nelas contidas.

5.2 - Abaixo são listados algumas das ferramentas mais populares para a disponibilização de serviços web (não apenas para web). Escolha duas delas e faça a mesma pesquisa da questão 5.1. Considerando, neste caso, as duas vulnerabilidades mais recentes, listadas com gravidade ***High*** ou ***Critical*** e que possuam *exploits* conhecidos.

* Joomla
* Wordpress
* Apache
* PHP
* JavaScript
* MySQL

5.3 - Em 2014 foi descoberta uma falha de programação na biblioteca de criptografia open source OpenSSL que ficou publicamente conhecida como *Heartbleed*. Esta falha foi identificada com CVE-2014-0160. Use esta identificação para descrever detalhadamente esta falha, incluindo (mas não apenas) as versões afetadas, os eventuais exploits existentes, vectores de ataque, impacto e soluções. Use as imagens de suas consultas e outros recursos utilizados para justificar suas conclusões.

5.4 - Em 16 de setembro de 2019 foi publicada uma vulnerabilidade afetando o popular gestor de *passwords* **LastPass**. Com base nos seus conhecimentos sobre bases de dados de vulnerabilidades, descreva detalhadamente a respectiva vulnerabilidade, assim como as fontes usadas para isso.

5.5 - Assim como diversas corporações, a Mozilla Foundation divulga informações sobre vulnerabilidades as quais os seus produtos foram expostos através do seu Security Advisories. Em 3 de setembro de 2019, a companhia disponibilizou uma atualização do seu browser, *i.e.*, Firefox ESR 68.1. Esta versão resolve uma série de vulnerabilidades listadas no relatório MFSA 2019-26. Descreva detalhadamente três vulnerabilidades listadas com gravidade ***Critical*** ou ***High***.