Atividade1

Charles Henrique Porto Ferreira
RA: 11103409

February 2015

1 Vulnerabilidades

Diversas são as vulnerabilidades que estão no nosso dia-a-dia. Desde pequenos aparelhos mobiles até navegadores web ou mesmo roteadores podem apresentar problemas de vulnerabilidades de seguranças que podem comprometer todo o sistema. Muitas destas vulnerabilidade são difíceis de serem detectadas e muitas vezes são usadas por pessoas mal intencionadas para executarem um ataque e tentarem derrubar o sistema, ou conseguir um acesso a algum shell para executar um comando ou mesmo acessar informações privilegiadas. As Subseções 1.1-1.7 mostram algumas desta vulnerabilidades e o que elas comprometem.

1.1 Sistemas ou Serviços de Sistemas Operacionais

- **GNU glibc CVE-2014-7817 Arbitrary Command Execution Vulnerability**

  Gnu glibc esta sucetível à vulnerabilidade que permite que pessoas que desejam atacar executem comandos arbitrários. Essas pessoas podem explorar estas vulnerabilidades para executar comandos arbitrários no contexto da aplicação afetada [12].
  Requisito comprometido: Integridade e Disponibilidade

- **CVE-2015-0421**
  Vulnerabilidade inesperada no Oracle java SE 8u25 permite que usuários locais afetarem confidencialidade, integridade e disponibilidade via vetores desconhecidos relacionados com o processo de instalação. De acordo com a Oracle: Aplica-se ao processo de instalação no cliente de *deployment* do Java [3].
  Requisito comprometido: confidencialidade, integridade e disponibilidade

- **CVE-2011-4103**
  emitter.py no Django Piston antes do 0.2.3 e 0.2.x antes do 0.2.2.1 não desserializa corretamente os dados YAML, os quais permitem que ataques

remotos executem código python arbitratiamente via vetores relacionados ao método yaml.load [5].
Requisito comprometido: Autenticidade, integridade, disponibilidade

1.2 Protocolos de Rede

- **CVE-2015-0586**
  O protocolo NetworkB-Based Apllication Recognition (NBAR) no Cisco IOS 15.3(100)M e anteriomente nos dispositivos Cisco 2900 Integrated Services Router (aka Cisco Internet Router) permitem que ataques causem uma queda do serviço (NBAR process hang) via pacotes IPv4, aka Bug ID CSCuo73682 [11].
  Requisito comprometido: Disponibilidade

1.3 Sistemas ou Serviços de Bancos de Dados

- **CVE-2014-7288**
  Syntantec PGP Universal Server and Encryption Management Server antes de 3.3.2 MP7 permite que autenticação remote de administradores executasse comandos shell via linha de comando em uma ação de restauração de backup de banco de dados [7].
  Requisito comprometido: integridade, disponibilidade

- **CVE-2015-0411**
  Vulnerabilidade inesperada no Oracle Mysql Server 5.5.40 e anteriores, e 5.6.21 e anteriores, permite que pessoas ataquem remotamante para afetar a confidencialidade, integridade e disponbilidade via vetores desocnhecidos relacionados ao Servidor: Segurança : Encruptação [10].
  Requisito comprometido: confidencialidade, integridade e disponbilidade

1.4 Navegadores Web (browsers)

- **CVE-2014-9648**
  componentes/intercepcao de navagacao/intercept_navigation_resource_throttle.cc no Google Chrmoe antes do 40.0.2214.91 no Android não restringe apropriadamente o uso intencional de URL para abrir aplicações após navegação em um web site, o que permite que ataques remotos causem uma queda do serviço (perca do acesso ao browser à aquele site) via códigos javascript, como demosntrado pelo pandora.com e pela Apliacaçao Pandora, uma vulnebailidade diferente da CVE-2015-1205 [9].
  Requisito comprometido: Disponibilidade

- **CVE-2009-4127**
  Vulnerabilidade Inesperada na extensão da Barra de Ferramentas do Wikipedia antes da 0.5.9.2 para o Firefox permitia que usuários executassem ataques

remotos arbitrarimaente via JavaScript com privrilegios Chrome usando vetores envolvendo botões não especificados na barra de ferramentas e a função eval. Nota: A proveniência desta informação é desconhecida; os detalhes foram obtidos por informação de fora [1].
Requisito comprometido: Disponibidade

- **CVE-2014-0322**
  Vulnerabilidade Use-after-free no Internet Explorer 9 e 10 permitem que ataques remotos executem código arbitrários via vetores envolvendo código JavaScript, Cmarkup, e o atributo onpropertychange de um elemento script, como exposto naturalmente em Janeiro e Fevereiro de 2014 [2].
  Requisito comprometido: Disponibilidade

1.5 Aplicativos que Manipulam Multimídia (imagens, vídeos, áudio, etc)

- **CVE-2014-8840**
  O compnente do Itunes Store no IOS da Apple 8.1.3 permite que ataques remotes bypass um mecanismo de proteção do Safari The iTunes Store component in Apple iOS before 8.1.3 allows remote attackers to bypass a Safari sandbox protection mechanism permitindo o redirenionamento de uma SSL URL para o iTunes Store [8].
  Requisito comprometido: Confidencialidade, autenticidade

1.6 Aplicativos de Produtividade Básica (editor, planilha, leitores de ebooks, etc)

- **CVE-2014-1350**
  Configurações do IOS da Apple 7.1.2 permite que atacantes fisicamente próximos bypass uma restrição de password do Icloud, e desligase o serviço Find My iPhone, ocasionando um gerencimaneto incorrento [4].
  Requisito comprometido: Autenticidade e confidencialidade

1.7 Equipamentos Eletrônicos (dispositivos de redes, dispositivos móveis ou controladores de dispositivos)

- **CVE-2014-7243**
  Roteador LG Electronic Mobile L-09C, L-03E, e L-04D não restringe o acesso par a interface de administração web, a qual permite que ataques remotos obtenha serviços de informação via vetores desconhecidos [6].
  Requisito comprometido: Confidencialidade

References

[1] National Vulnerability Database. Cve-2009-4127. https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-4127.

[2] National Vulnerability Database. Cve-2014-0322. https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0322.

[3] National Vulnerability Database. Cve-2014-0421. https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0421.

[4] National Vulnerability Database. Cve-2014-1350. https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-1350.

[5] National Vulnerability Database. Cve-2014-4103. https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4103.

[6] National Vulnerability Database. Cve-2014-7243. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7243.

[7] National Vulnerability Database. Cve-2014-7288. https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7288.

[8] National Vulnerability Database. Cve-2014-8840. https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-8840.

[9] National Vulnerability Database. Cve-2014-9648. https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-9648.

[10] National Vulnerability Database. Cve-2015-0411. https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0411.

[11] National Vulnerability Database. Cve-2015-0586. https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0586.

[12] Security Focus. Cve-2014-7817. http://www.securityfocus.com/bid/71216/discuss.