Revista EduFatec: educação, tecnologia e gestão
V.2 N.1 - janeiro-junho/2019

VULNERABILIDADES DE SEGURANÇA EM DISPOSITIVOS ANDROID: ANÁLISES E ESTATÍSTICAS (2009 – 2019)

Fernanda Ribeiro do Nascimento[1]

Fausto Gonçalves Cintra[2]

Resumo

A segurança da informação tem se tornado a cada dia mais relevante devido ao grande avanço tecnológico vivenciado não apenas por empresas, mas também por pessoas que utilizam dos recursos de tecnologia em sua vida pessoal e profissional. O crescimento exponencial do uso de dispositivos móveis para fins pessoais, profissionais e mesmo financeiros traz consigo a preocupação de se garantir que os dados particulares de cada usuário estejam devidamente seguros. O presente trabalho tem como objetivo realizar uma análise das vulnerabilidades de segurança em dispositivos móveis que se utilizaram do sistema operacional Android entre os anos de 2009 e 2019. Para tal, busca em bases de dados online informações pertinentes ao tema, tais como a quantidade, o tipo e a incidência das vulnerabilidades existentes. As estatísticas indicam que as versões desatualizadas do sistema operacional Android se tornam mais susceptíveis a vulnerabilidades de segurança do que versões mais atuais do mesmo sistema operacional. Indicam, ainda, que a instalação de aplicativos de reputação duvidosa ou desconhecida pode prejudicar a segurança dos dados e as informações dos usuários.

Palavras-chave: Ameaças. Ataques. Elevação de privilégios. Execução remota de código. Furto de identidade. Segurança da Informação.

Abstract

Information security has become more and more relevant due to the great technological advance experienced not only by companies, but also by people who use the technology resources in their personal and professional life. The exponential growth of the use of mobile devices for personal, professional and even financial purposes brings along the concern of ensuring the security of each user's particular data. This paper aims at performing an analysis of security vulnerabilities in mobile devices that used the Android operating system between the years 2009 and 2019. For that, online databases for information relevant to the subject were searched for the quantity, the type and the incidence of the existing vulnerabilities. Statistics indicate that outdated versions of the Android operating system has become more susceptible to security vulnerabilities than more current versions of the same operating system. Furthermore, they point out that installing unknown applications with questionable reputation can harm data security and user's information.

[1] Graduanda em Análise e Desenvolvimento de Sistemas pela Fatec Dr. Thomaz Novelino – Franca/SP. Endereço eletrônico: fer.r.n@hotmail.com

[2] Docente da Fatec Franca, Mestre em Desenvolvimento Regional pelo Centro Universitário Municipal de Franca, Bacharel em Ciência da Computação com ênfase em Análise de Sistemas pela Universidade de Franca. Endereço eletrônico: fausto.cintra@fatec.sp.gov.br

ISSN: 2595-5942

Keywords: *Attacks. Elevation of privileges. Identity theft. Remote Code Execution. Security of Information. Threats.*

1 Introdução

Atualmente, utiliza-se cada vez mais de sistemas informatizados para a realização de diversas atividades, tornando os sistemas mais integrados com bases de dados por meio de redes. Acompanhado do crescimento exponencial do uso da tecnologia e sistemas informatizados por diversos tipos de pessoas e organizações, o universo digital se tornou também sujeito a diversas formas de ameaças físicas e virtuais, que "comprometem seriamente a segurança das pessoas e das informações a elas atinentes, bem como das transações que envolvem o complexo usuário-sistema-informação" (MARCIANO, 2006. p. 16).

A disseminação massiva de acesso à informação por meio da informática e proliferação da internet e de redes corporativas facilita e agiliza a utilização de recursos computacionais. Contudo, expõe mais ainda os riscos e a fragilidade a que estão expostos os usuários, os dados armazenados e os sistemas que utilizam para tratar esses dados (MARCIANO, 2006). A preocupação com segurança das informações deve ser um item obrigatório para a implementação de sistemas.

Nos últimos anos, o mercado de *smartphones* cresceu de maneira que os dispositivos são usados a todo momentos em diversos contextos, seja casualmente em família, no dia-a-dia ou em empresas e grandes organizações. Isso pode representar inúmeros riscos de invasão a redes e sistemas, assim como vazamento de informações particulares ou sigilosas (ALMEIDA, 2013).

O presente estudo tem como objetivo analisar as vulnerabilidades de segurança de informação presentes em dispositivos móveis que utilizaram o sistema operacional Android nos últimos dez anos (2009 a 2019). Serão utilizados os parâmetros oferecidos pelas bases de dados *online* Android Vulnerabilities (2019) e CVE Details (2019), além dos dados disponíveis no boletim de segurança do Android, publicado pela Android Source (2019).

2 Referencial teórico e trabalhos correlatos

Informação é um bem que precisa ser protegido, que demanda segurança. Portanto, serão abordados neste tópico os temas de segurança da informação, suas

vulnerabilidades e ameaças, assim como os dispositivos Android e suas características.

2.1. Segurança da Informação

Informação é muito mais do que um conjunto de dados, é um bem de valor pessoal ou profissional e que deve ser protegido. Portanto, há normas de segurança da informação que definem regras e valores que os administradores ou indivíduos que possuem acesso à informação devem seguir. A segurança da informação se torna mais importante à medida que indivíduos e organizações possuem suas informações armazenadas, processadas e disponibilizadas no ambiente computacional (FONTES, 2003). As políticas de segurança da informação são "apresentadas como códigos de conduta aos quais os usuários dos sistemas computacionais devem se adequar integralmente" (MARCIANO, 2006. p. 109).

Os pilares da segurança da informação podem ser resumidos em: confidencialidade, integridade e disponibilidade (ABNT, 2013).

- Confidencialidade diz respeito ao uso autorizado da informação, ou seja, classificação da informação e controle de acesso a ela.
- Integridade refere-se à manutenção de valores e características originais da informação por meio de alterações permitidas, controladas e identificadas, de maneira a evitar alterações indevidas ou perda de seu valor.
- Disponibilidade implica em prover a informação no tempo, local e da maneira em que for necessária.

Dessa maneira, a segurança se faz presente no universo computacional, inserindo-se em todos os níveis. Porém, pode-se observar um número crescente de incidentes relativos à segurança da informação, como furtos de senhas, fraudes digitais, vírus e outras ameaças. Um incidente de segurança é definido como um evento adverso relacionado à segurança de sistemas ou redes de computadores. As vulnerabilidades, ou falhas de mecanismos computacionais, quando exploradas, dão ocorrência aos incidentes (MARCIANO, 2006).

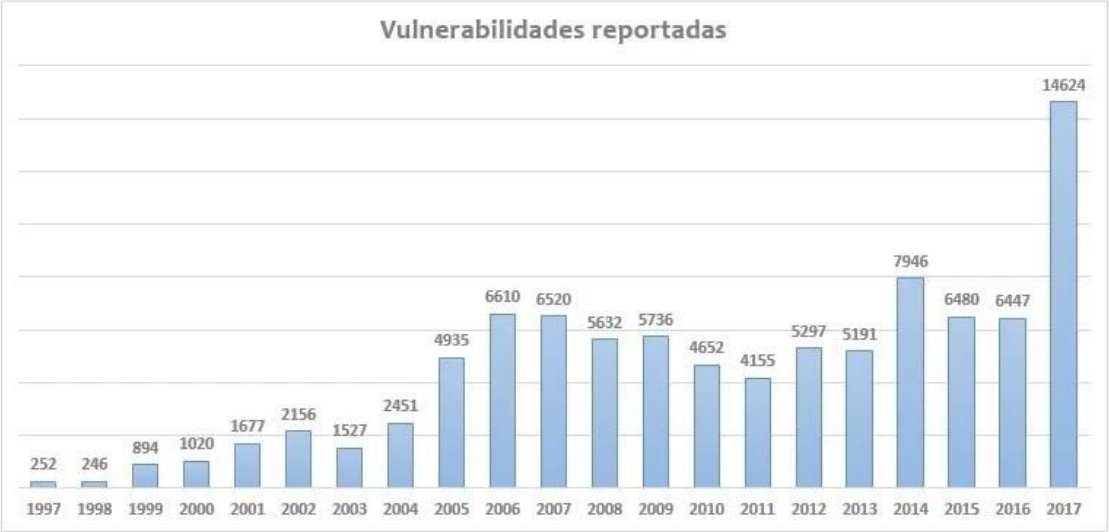
2.2. Vulnerabilidades de segurança da informação - Conceitos, características, históricos e estatísticas

É possível dizer que uma vulnerabilidade surge quando há uma fraqueza nas medidas de proteção de um sistema computacional podendo ser explorada por um usuário ou mecanismo mal-intencionado. A partir das vulnerabilidades, é possível realizar um mapeamento crítico para onde são apontados os ataques, aos quais um sistema possa estar susceptível.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) define um incidente de segurança como toda situação ou evento adverso em que um sistema ou entidade de informação é colocado sob risco, seja comprometido ou sob suspeita (CERT.br, 2017).

Observa-se um crescimento ao longo das últimas décadas no número de ocorrências de incidentes e vulnerabilidades relacionados à segurança, como fraudes digitais, furtos de senhas, vírus e outras ameaças. Na Figura 1 apresenta-se o aumento do número de vulnerabilidades em mecanismos computacionais na América Latina, principalmente no ano de 2017.

Figura 1 – Vulnerabilidades de segurança da informação reportados no período de 1997 a 2017.



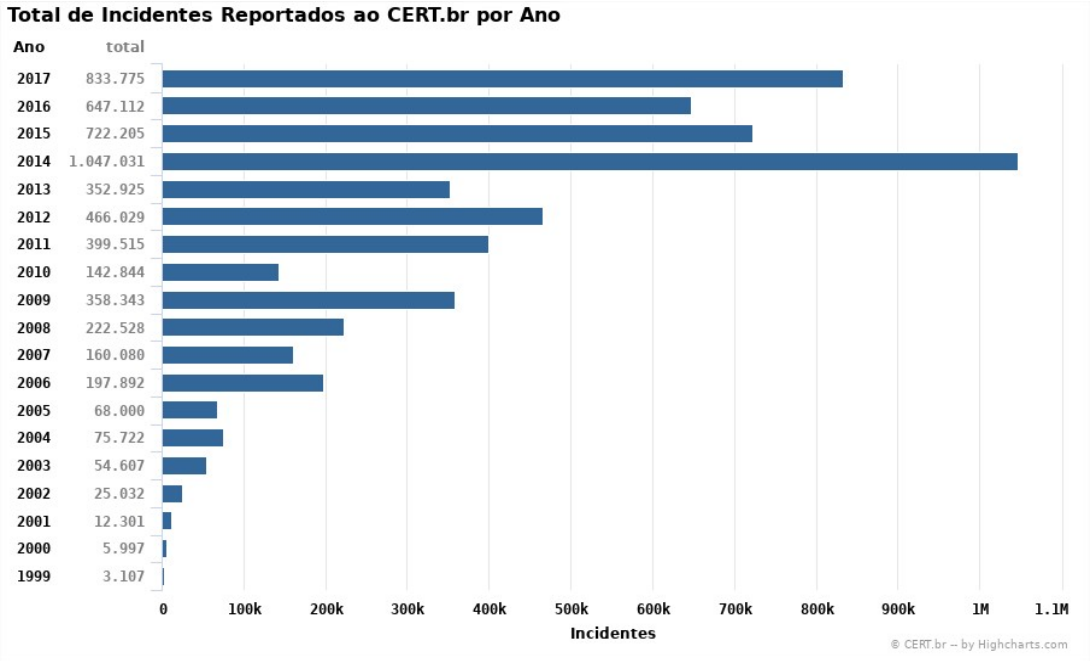
Fonte: Conteúdo Editorial (2018), online.

A Figura 2 demostra o número de incidentes de segurança no Brasil reportados entre os anos 1999 e 2017 ao CERT.br.

ISSN: 2595-5942

Revista EduFatec: educação, tecnologia e gestão
V.2 N.1 - janeiro-junho/2019

Figura 2 – Incidentes de Segurança da Informação entre 1999 e 2017.



Fonte: CERT.br (2018), online.

Os incidentes reportados no ano de 2017 foram classificados nas seguintes categorias (tipos de ataques), conforme apresentado na Figura 3: *worm,* DoS, invasão, *Web, Scan,* fraude e outros.

Figura 3 – Categorias dos incidentes de segurança reportados no ano de 2017.

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2017

Tabela: Totais Mensais e Anual Classificados por Tipo de Ataque.

Mês	Total	worm (%)		dos (%)		invasão (%)		web (%)		scan (%)		fraude (%)		outros (%)	
jan	**64161**	1119	1	154	0	62	0	12169	18	44475	69	5424	8	758	1
fev	**27092**	1469	5	76	0	35	0	4362	16	16809	62	3815	14	526	1
mar	**54305**	1391	2	19	0	23	0	6281	11	41423	76	4587	8	581	1
abr	**51011**	2086	4	29	0	18	0	7782	15	35530	69	5310	10	256	0
mai	**47616**	2100	4	8	0	50	0	6232	13	32858	69	6027	12	341	0
jun	**49519**	3949	7	237	0	14	0	8320	16	30959	62	5733	11	307	0
jul	**257618**	4973	1	207780	80	1	0	4131	1	34364	13	5559	2	810	0
ago	**54035**	4110	7	11314	20	23	0	3037	5	28592	52	6513	12	446	0
set	**47940**	7264	15	254	0	24	0	1465	3	35474	74	3308	6	151	0
out	**74116**	7350	9	184	0	13	0	1691	2	60890	82	3690	4	298	0
nov	**63646**	5253	8	120	0	39	0	3245	5	51466	80	3316	5	207	0
dez	**42716**	4037	9	13	0	99	0	2051	4	30418	71	6037	14	61	0
Total	**833775**	45101	5	220188	26	401	0	60766	7	443258	53	59319	7	4742	0

Fonte: CERT.br (2018), online.

ISSN: 2595-5942

Revista EduFatec: educação, tecnologia e gestão
V.2 N.1 - janeiro-junho/2019

2.3 Ameaças

Ameaças são eventos ou ações indesejáveis que desabilitam, removem, danificam ou destroem recursos (MARCIANO, 2006). Elas se utilizam de vulnerabilidades de segurança da informação, *bugs* de sistema ou usuário, para obter acesso não autorizado a informações ou recursos, possibilitando a revelação não autorizada de informações.

São doze as categorias de potenciais ameaças, segundo Marciano (2006), dispostas a seguir de acordo com o grau de severidade:

1. Eventos cometidos com uso de *softwares* (vírus, vermes, macros, negação de serviço);
2. Erros ou falhas técnicas de *softwares* (falhas de codificação, *bugs*);
3. Falhas ou erros humanos (acidentes, enganos);
4. Atos deliberados de invasão ou espionagem, *hacking;*
5. Atos deliberados de sabotagem ou vandalismo (destruição de sistemas ou informação);
6. Erros ou falhas técnicas de *hardware* (falhas de equipamentos);
7. Atos deliberados de furto (de equipamento ou informação);
8. Forças da natureza (terremotos, enchentes, relâmpagos, incêndios não intencionais);
9. Comprometimento à propriedade intelectual (pirataria, infração a direitos autorais);
10. Variação da qualidade de serviço (*Quality of Service - QoS*) por parte dos provedores, como energia elétrica e serviços de redes de comunicação;
11. Obsolescência técnica;
12. Atos deliberados de extorsão da informação (chantagem ou revelação indevida de informação).

Ameaças de segurança da informação podem ocasionar o que é chamado de evento. Um evento é a “ocorrência identificada de procedimento, sistema, serviço ou rede que indica possível perda de controle ou violação da política de segurança da informação, ou situação desconhecida que possa ser relevante para a segurança da informação” (EBSERH, 2017. p. 6).

Dentre as ameaças encontradas em dispositivos Android estão: p*hishing, trojans, spyware, bots, root exploits,* fraude via SMS, *premium dealers* e falsos

ISSN: 2595-5942

instaladores (ALMEIDA, 2006). As ameaças tornam possíveis ataques aos dispositivos vulneráveis. Segundo Lepesqueur e Oliveira (2012), um ataque consiste em qualquer ação que possivelmente comprometa a segurança das informações de um sistema. Os ataques são a maneira mais clara de se avaliar o potencial crítico de uma falha de segurança. São classificados de acordo com três parâmetros: (1) os resultados que produzem, (2) a forma em que são praticados e (3) o ponto de vista da rede.

Quanto aos resultados que produzem, são divididos em quatro categorias (LEPESQUEUR; OLIVEIRA, 2012):

- Interrupção: desativam serviços, submetendo-os à reinicialização;
- Interceptação: o atacante se posiciona entre dois computadores da rede e se passa por um dos computadores originais, obtendo uma conexão que permite leitura ou modificação dos dados trocados entre os *hosts* originais;
- Modificação: o atacante terceiro obtém acesso não autorizado a determinados recursos do sistema, podendo modificar informações ou configurações;
- Fabricação: compromete-se a autenticidade do sistema burlando o processo de confirmação ao receptor de que a mensagem procede realmente da origem informada.

Quanto à forma como são praticados os ataques, classifica-se em duas categorias: passivo, na qual não há alteração na informação e no fluxo normal do canal, apenas ocorre o monitoramento das mensagens circulantes na rede e coleta de informações; e ativo, na qual promove-se intervenção no fluxo normal de informações, alteração de conteúdo ou produção de informações falsas, de modo a atentar contra a segurança do sistema (LEPESQUEUR; OLIVEIRA, 2012).

Referente à rede, os ataques são divididos em ataques internos e externos. Os ataques internos ocorrem quando o invasor já está dentro da rede e têm como característica uma constante elevação de privilégios, a fim de se obter o maior nível de privilégios possíveis. Os ataques externos são “ataques em profundidade” (LEPESQUEUR; OLIVEIRA, 2012. p. 6), visto que o objetivo é superar a infraestrutura externa que isola a rede interna do mundo externo.

Os principais atacantes de usuários de dispositivos móveis são (ALMEIDA, 2013):

ISSN: 2595-5942

Revista EduFatec: educação, tecnologia e gestão
V.2 N.1 - janeiro-junho/2019

- *Hackers:* indivíduos que à primeira vista aparentam ser uma ameaça, por serem capazes de infiltrarem sem autorização por cada parte de um sistema, podendo inclusive modificar as partes do sistema, porém com o intuito de melhorar, notificando o responsável pelo sistema. O termo *hacker* pode ser ainda subdividido em *hacker white hat*, sendo este o *hacker* ético*; hacker gray hat*, que se infiltra em sistemas sem autorização, porém sem intenção de roubo, e *hacker black hat* ou *cracker.*
- *Cracker:* Seu intuito é cometer crimes virtuais e possui, assim como os *hackers*, um vasto conhecimento de informática. Geralmente trabalha em conjunto com outros *crackers.*
- *Phreackers*: têm o intuito de invadir telefonia móvel, fixa e pública, a fim de utilizar dos serviços sem cobrança em valor monetário.

2.4 Dispositivos Android – características, serviços, ferramentas

Dispositivos móveis, como celulares, *smartphones* e *tablets*, têm se tornado cada vez mais capazes de executar grande parte das ações realizadas em computadores pessoais, como navegação *web, internet banking* e acesso a *e-mails* e redes sociais. Dessa forma, os dispositivos móveis também podem ser usados para a prática de atividades maliciosas, como furto de dados, envio de *spam*, propagação de códigos maliciosos e disparo de ataques na *Internet*.

Além desses riscos, os dispositivos móveis possuem características próprias que os tornam mais atraentes para indivíduos ou mecanismos mal-intencionados, como a grande quantidade de informações pessoais armazenadas, maior possibilidade de perda ou furto, diversas aplicações desenvolvidas por terceiros e rapidez na substituição dos modelos (MENDES, 2017).

O sistema operacional Android tem como característica principal a sua natureza *open source*, ou seja, de código aberto. Isso possibilita a implementação por parte das empresas de suas próprias funcionalidades de *hardware* ou *software*. Um grande problema trazido por esse meio *open source* são as atualizações, que se contiverem falhas podem ocasionar fragmentação de versões do sistema e assim deixar um maior número de dispositivos vulneráveis. Somado a esse fator, diversos desenvolvedores disponibilizam seus aplicativos diariamente na loja de aplicativos do Android (PlayStore), muitos desses sendo vulneráveis a ataques que possibilitam

ISSN: 2595-5942

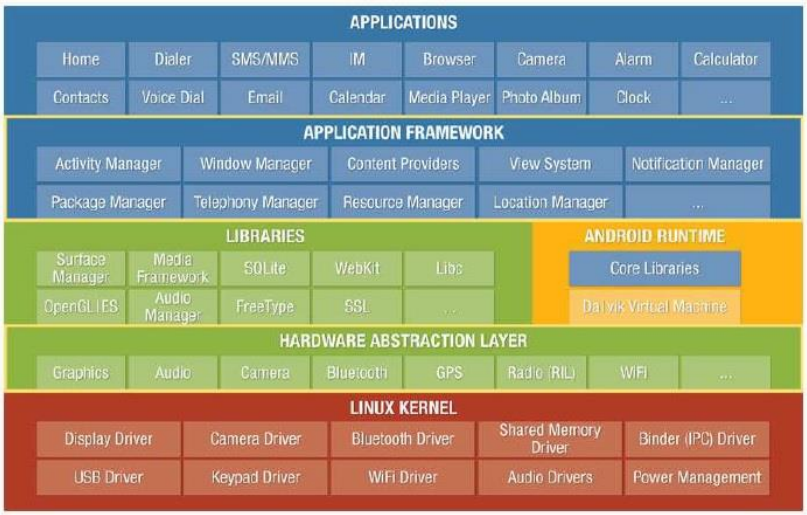
acesso não autorizado, roubo de informações particulares, *spam* e/ou outros tipos de ameaças ao usuário ou empresa (MENDES, 2017).

Segundo Amaral et al (2017), muitas pessoas acreditam ter segurança em seus dispositivos móveis enquanto navegam na Internet. Entretanto, a instalação de diversos *apps*, sem o conhecimento das permissões necessárias para o seu funcionamento ou até mesmo suas funcionalidades, acabam executando processos em segundo plano que podem obter acesso a dados e informações no dispositivo, sem percepção do usuário.

2.4.1 Arquitetura Android

A arquitetura de sistemas Android é dividida nos componentes a seguir, do mais interno ao mais externo: *kernel linux*, camada de abstração de *hardware*, bibliotecas auxiliares, Android *runtime*, *framework* de aplicação e aplicativos (Figura 4). Conhecer os principais componentes da plataforma é importante tanto para o desenvolvimento *mobile* quanto para identificar vulnerabilidades nas aplicações (MENDES, 2017).

Figura 4 – Arquitetura do sistema operacional Android



Fonte: Agrawal (2016), online.

A camada de *kernel* consiste no núcleo, portanto sendo essencial para gerenciamento de memória e processos do sistema, rede, *drivers*, segurança e controle de acesso a arquivos e pastas. No Android, o *kernel* foi projetado com base na versão 2.6 do *kernel* do Linux, sendo semelhante em suas funcionalidades,

Revista EduFatec: educação, tecnologia e gestão
V.2 N.1 - janeiro-junho/2019

segurança, gestão de memória e gestão de processos (LEITE; REIS, 2017). Logo acima está a camada de abstração de *hardware* (HAL), que fornece acesso a recursos de *hardware* por meio da comunicação entre o *kernel* e outros níveis acima dele. A camada seguinte, a de bibliotecas, refere-se à camada nativa, pois os códigos ali escritos em C e C++ são otimizados para rodar sobre o *hardware* do Android. O acesso a essa biblioteca por meio de desenvolvedores se faz por meio de uma interface humana chamada *Java Native Interface (JNI)*, que liga as bibliotecas a camada de aplicação (MENDES, 2017).

O desenvolvimento para aplicativos se dá na linguagem Java (ou na linguagem Kotlin, a partir da versão Oreo 8.0 do sistema operacional, com 100% de interoperabilidade com Java e Android), porém o sistema operacional não utiliza máquina virtual que executa códigos Java, mas sim uma máquina otimizada para dispositivos móveis, chamada *Android Runtime* (ART), com melhor responsividade à Interface do Usuário (UI). Por meio dos processos de compilação de arquivos Java se obtêm arquivos com extensão .class, que contêm código Java executável em *Java Virtual Machine* (JVM), os quais são recompilados para formato .dex, executável pela máquina virtual do Android. Após esse processo, os arquivos são compactados em um arquivo no formato apk (*Android Package Kit*), que representa a versão a ser distribuída e instalada em dispositivos Android. Em seguida, a camada de *framework* de aplicação, onde fica o *kit* de desenvolvimento de software Android (Android SDK), disponibiliza módulos para construção de aplicações. Os mais importantes módulos consistem em (MENDES, 2017):

- *Views*: providencia a interface do usuário;
- *Resource Manager*: gerenciador de acesso aos recursos;
- *Notification Manager:* permite responder a eventos em forma de notificações personalizadas;
- *Activity Manager:* gerenciador de ciclo de vida de determinada aplicação;
- *Content Providers:* permitem que as aplicações compartilhem dados entre si.

Finalmente, a camada mais externa, que se refere às aplicações do sistema (*e-mail*, mapas, *player* de áudios, contatos telefônicos, etc.) e aplicativos desenvolvidos por terceiros, adquiridos oficialmente pela loja Google Play ou outros mercados para Android, de maneira não oficial. As aplicações são identificadas por um *package*, ou pacote, de maneira única e individual. Caracteriza-se por executar

ISSN: 2595-5942

Revista EduFatec: educação, tecnologia e gestão
V.2 N.1 - janeiro-junho/2019

as aplicações sobre a plataforma, sendo elas nativas do sistema ou desenvolvidas por terceiros (LEITE; REIS, 2017).

2.4.2 Vulnerabilidades do Android

Mendes (2017) descreve em seu trabalho a categorização de vulnerabilidades no Android da seguinte maneira:

1. Uso inapropriado da plataforma: refere-se ao mal-uso ou falhas de controles de segurança. Pode ser o mal-uso de permissões ou chamadas à API (*Application Programming Interface* – Interface de Programação de Aplicativos) de terceiros ou ainda controles de segurança como *keychain* (chaves de acesso privadas);
2. Armazenamento inseguro de dados: consiste no armazenamento de dados de maneira insegura ou o vazamento dos dados de forma não intencional. No Android pode ocorrer por meio de banco de dados SQLite, logs, XMLs com dados ou cartões SD.
3. Comunicação insegura: corresponde aos problemas no tráfego de rede do aplicativo, geralmente por falta de proteção aos dados trocados com o servidor;
4. Autenticação insegura: remete aos controles de autenticação falhos, dando margem à execução de métodos no *backend* da aplicação, justamente por não saber se o usuário estará *online* ou *offline;*
5. Criptografia insuficiente: o código aplica criptografia em informações sensíveis, porém de forma insuficiente para proteger as informações;
6. Autorização insegura: o aplicativo não distribui de forma correta as decisões de autorização, permitindo, dessa forma, que usuários com menos privilégio executem funções de alto privilégio em modo *offline;*
7. Qualidade do código: problemas relacionados a nível de implementação do código do lado do cliente, como *buffer overflow* (ocorre quando o aplicativo tenta gravar dados além do que o *buffer* de memória permite, assim sobrecarregando o sistema);
8. Adulteração de código: modificação do código e dados do aplicativo por parte do atacante de modo a obter vantagens pessoais ou monetárias;
9. Engenharia reversa: revelação de código fonte, análise de código binário ou outros recursos a nível de código da aplicação;

ISSN: 2595-5942

Revista EduFatec: educação, tecnologia e gestão
V.2 N.1 - janeiro-junho/2019

10. Funcionalidade estranha: funcionalidades utilizadas em versões de teste estão, acidentalmente, na versão de lançamento da aplicação.

3 Metodologia de Desenvolvimento

As vulnerabilidades em dispositivos Android foram analisadas nessa pesquisa, em um período de 10 anos (2009 a 2019) utilizando resultados e estatísticas providas pelas bases de dados *online* Android Vulnerabilities (2019) e CVE Details (2019). Foram também descritas as estatísticas adquiridas pelo boletim oficial de segurança do Android, publicado por Android Source (2019). Uma vez que nenhuma dessas bases, utilizadas como fonte de dados secundários (MARCONI; LAKATOS, 2003), abrange todo o período estudado (2009—2019), foi necessário avaliar qualitativamente as vulnerabilidades mais destacadas durante a época coberta por cada uma delas.

3.1 Análise de vulnerabilidade em dispositivos Android – conceitos, ferramentas e aplicação

Existem, segundo Mendes (2017), dois tipos de análises para códigos em geral, a *white-box testing*, na qual o código fonte já é aberto para testes e se pode ver as funções, variáveis e métodos; e a *black-box testing*, na qual não se tem acesso ao código fonte. A diferença, no Android, não é tão grande pois os aplicativos podem ser descompilados para códigos similares aos originais. Os descompiladores têm a função de transformar códigos de alto nível para códigos de máquina e transformarem novamente código de máquina para código de alto nível.

Para analisar aplicativos Android existem dois tipos de ferramentas, podendo ser de análise estática (executada quando há acesso ao APK, porém sem execução do aplicativo no momento, para verificar potenciais problemas que podem surgir quando o aplicativo for executado) ou dinâmica (analisa com o aplicativo em execução, de forma a monitorar mudanças em tempo real, arquivos do sistema e comunicações ponto-a-ponto) (MENDES, 2017).

Para este estudo, foram analisadas as estatísticas apresentadas por Android Vulnerabilities (2019). Os pesquisadores Daniel Thomas, Alastair Beresford, Andrew Rice e Daniel Wagner criaram, na Universidade de Cambridge, no laboratório de

ISSN: 2595-5942

Revista EduFatec: educação, tecnologia e gestão
V.2 N.1 - janeiro-junho/2019

computação, o escore FUM para comparar a segurança provida por diferentes dispositivos Android, de diferentes fabricantes. O escore designa a cada fabricante de dispositivos que utilizam Android uma pontuação até 10 com base na segurança que os fabricantes ofereceram aos seus consumidores pelos anos de 2011 a 2015.

O escore é composto por três itens:

- ***F:*** representa a proporção de dispositivos livres de vulnerabilidades críticas conhecidas;
- ***U:*** compreende a proporção de dispositivos atualizados para a sua versão mais recente de Android;
- ***M:*** abrange o número de vulnerabilidades que o fabricante ainda não corrigiu em nenhum dispositivo.

A Figura 5 demonstra a fórmula utilizada pelos pesquisadores para calcular o escore FUM.

Figura 5 – Fórmula do FUM score

$$FUM\,score = 4 \cdot f + 3 \cdot u + 3 \cdot \frac{2}{1+e^{m}}$$

Fonte: Android Vulnerabilities (2019), online.

Foram utilizadas ainda, nessa pesquisa, as estatísticas e resultados apresentados por CVE Details (2019), que consiste em uma base de dados de segurança e vulnerabilidades. CVE (*Common Vulnerabilities and Exposures* ou vulnerabilidades e exposições comuns) consiste em uma lista de nomes padronizados para vulnerabilidades e informações sobre exposições à segurança (GFI LANGUARD, 2016). O site disponibiliza uma interface *web* para visualizar dados referentes a vulnerabilidades de segurança adquiridos no *National Vulnerability Database* (NVD) ou Banco de Dados de Vulnerabilidades Nacional dos Estados Unidos, que são providos pelo *National Institute of Standards and Technology* (Instituto Nacional de Padrões e Tecnologia). Os dados apresentados nesta pesquisa são do período de 2009 a 2018.

Por fim, para realizar uma análise das vulnerabilidades de segurança mais recente, foi consultado o Android Source (2019), que contém detalhes de

 ISSN: 2595-5942

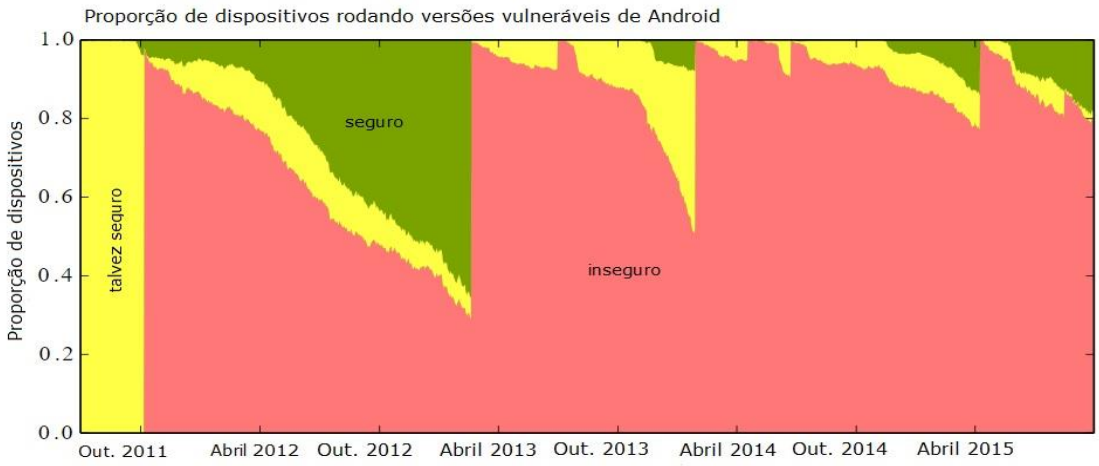
Revista EduFatec: educação, tecnologia e gestão
V.2 N.1 - janeiro-junho/2019

vulnerabilidades de segurança que afetam dispositivos Android. Foram analisados os detalhes para cada uma das vulnerabilidades de segurança que se aplicam ao nível do *patch* (ou correção) realizado em 01/03/2019.

4 Levantamento de dados

Android Vulnerabilities (2019) apresenta um gráfico (Figura 6) que demonstra a proporção de dispositivos rodando versões vulneráveis de Android.

Figura 6 – Proporção de dispositivos rodando versões vulneráveis de Android durante os anos 2011 a 2015.



Fonte: adaptado de Android Vulnerabilities (2019), online.

A figura demonstra a estimativa feita pelos pesquisadores categorizando em **seguro**, **talvez seguro** e **inseguro**, as versões de Android ao longo desses anos. Para que um dispositivo seja considerado **inseguro** foram consideradas duas condições: (1) o dispositivo está executando uma versão de Android que está há pelo menos um ano vulnerável a uma das vulnerabilidades listadas a seguir; e (2) o dispositivo não passou por atualização que corrige a vulnerabilidade.

Para considerar um dispositivo como **talvez seguro**, o dispositivo deveria estar rodando uma versão de Android que é vulnerável a pelo menos uma das vulnerabilidades listadas abaixo ou o dispositivo deve ter recebido uma atualização que possivelmente corrigiria a vulnerabilidade.

Os dispositivos considerados como **seguro** estariam executando versões de Android que não são afetadas por nenhuma das vulnerabilidades listadas.

ISSN: 2595-5942

Revista EduFatec: educação, tecnologia e gestão
V.2 N.1 - janeiro-junho/2019

Foram considerados dados de 21.713 dispositivos que participaram do estudo *Device Analyzer,* aplicativo desenvolvido pela Universidade de Cambridge que permite ao usuário obter estatísticas sobre o seu dispositivo e as coletar para pesquisas científicas. O aplicativo colheu dados a partir das informações de uso do dispositivo, periodicamente salvando esses dados no servidor da Universidade de Cambridge, possibilitando aos pesquisadores da Universidade agregar com dados de outros usuários e desenhar as estatísticas referentes aos dados pesquisados (ANDROID VULNERABILITIES, 2019).

Os pesquisadores do escore FUM acreditam que os dados obtidos utilizando o aplicativo *Device Analyzer* proporcionam uma visão otimista da segurança em dispositivos Android pois o aplicativo executa a versão mais recente do sistema operacional.

As 14 vulnerabilidades utilizadas na pesquisa para traçar o gráfico da Figura 7 estão listadas abaixo seguidas pela data em que foram descobertas ou corrigidas:

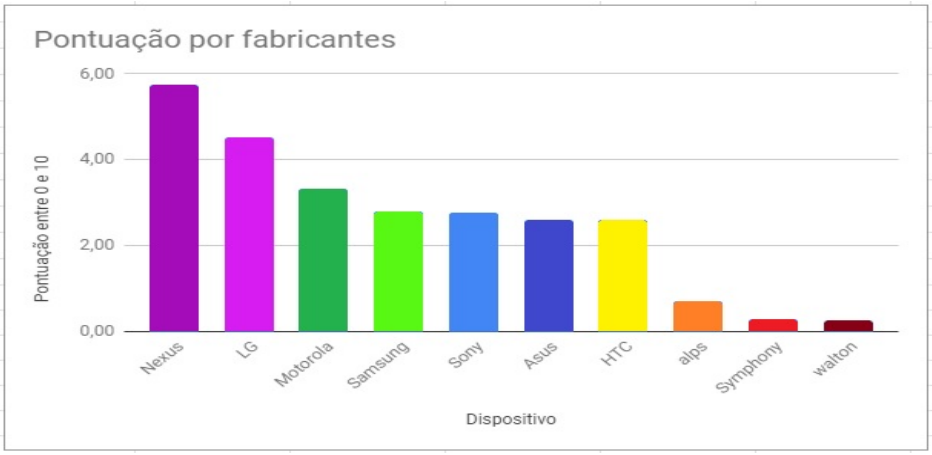
1. KillingInTheNameOf psneuter ashmem – 13/07/2010
2. Exploit udev – 15/07/2010
3. Levitator – 10/03/2011
4. Gingerbreak – 18/04/2011
5. zergRush – 06/10/2011
6. APK duplicate file – 18/02/2013
7. APK unchecked name – 30/06/2013
8. APK unsigned shorts – 03/07/2013
9. Fake ID – 17/04/2014
10. TowelRoot – 03/05/2015
11. ObjectInputStream deserializable – 22/06/2014
12. Stagefright – 08/04/2015
13. One class to rule them all – 22/05/2015
14. Stagefright2 – 15/08/2015

Os pesquisadores do método FUM analisaram também os escores até a pontuação 10 de fabricantes de dispositivos móveis que utilizam Android e dispositivos Nexus. Os resultados estão apresentados no gráfico a seguir (Figura 7).

ISSN: 2595-5942

Revista EduFatec: educação, tecnologia e gestão
V.2 N.1 - janeiro-junho/2019

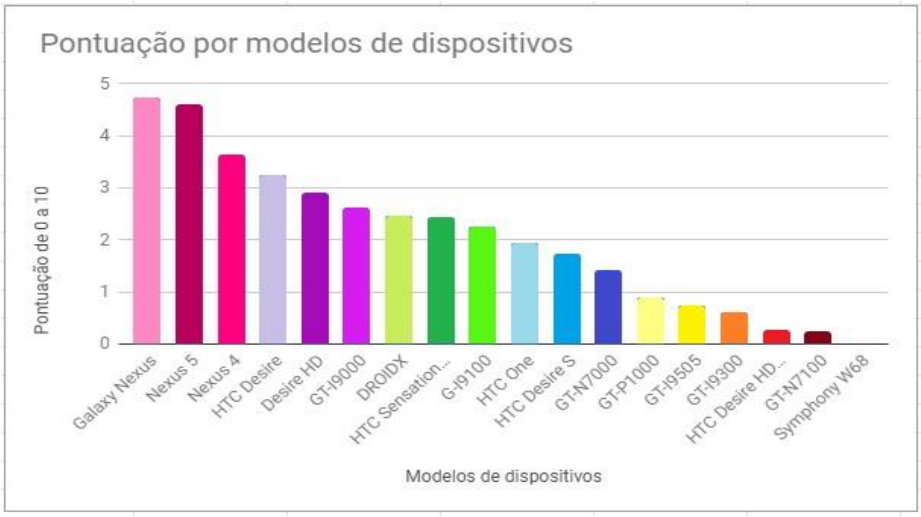
Figura 7 – Escore por fabricantes de dispositivos Android ou Nexus, utilizando o escore FUM



Fonte: adaptado de Android Vulnerabilities (2019), online.

Foram analisados também os modelos dos dispositivos, aplicando o escore FUM para avaliar até pontuação 10. A seguir serão apresentados os resultados na figura 8.

Figura 8 - Escore por modelos de dispositivos de fabricantes Android ou Nexus, utilizando o escore FUM.



Fonte: adaptado de Android Vulnerabilities (2019), online.

Já a pesquisa realizada no banco de dados do CVE Details (2019) indicou resultados de tendências de vulnerabilidades ao longo dos anos, assim como a ocorrência de vulnerabilidades por ano e por tipo. Os resultados são apresentados a seguir nas Figuras 9, 10 e 11.

ISSN: 2595-5942

Revista EduFatec: educação, tecnologia e gestão
V.2 N.1 - janeiro-junho/2019

Figura 9 – Número de vulnerabilidades registradas por ano.

Fonte: adaptado de CVE Details (2019), online.

Figura 10 – Número de vulnerabilidades registradas por cada tipo

Fonte: adaptado de CVE Details (2019), online.

Figura 11 – Maiores vulnerabilidades ocorridas ao longo do tempo

Ano	Nº de vulnerabilidades	DoS	Execução de código	Overflow	Corrupção de memória	SQL injection	XSS	Diretório Transversal	Divisão de respostas HTTP	Bypass Something	Ganho de informações	Ganho de privilégios	CSRF	Inclusão de arquivos	Nº de exploits
2009	5	3								1					
2010	1	1	1												
2011	9	1	1		1					3	2	3			
2012	8	5	4	2							1				1
2013	7	1	2	2	2					1	1	3			
2014	13	2	4	1		1				1	2	2			1
2015	125	56	70	63	46					20	19	17			
2016	525	106	73	92	38					48	99	250			
2017	842	87	206	162	32			1		31	115	36			
2018	611	32	84	150	12	3	1	1		17	64	3			
Total	2146	294	445	472	131	4	1	2		122	303	314			2
% de todos		13,7	20,7	22	6,1	0,2	0	0,1	0	5,7	14,1	14,6	0	0	

Fonte: adaptado de CVE Details (2019), online.

A seguir, é possível observar a análise dos dados apresentados por Android Source (2019), que apresentam detalhes sobre todas as vulnerabilidades

ISSN: 2595-5942

Revista EduFatec: educação, tecnologia e gestão
V.2 N.1 - janeiro-junho/2019

encontradas em dispositivos Android que passaram por correções em 01/03/2019 e 05/03/2019. As vulnerabilidades foram agrupadas de acordo com o componente que elas afetam, apresentando a descrição do problema e uma tabela com o CVE, referências associadas, tipo de vulnerabilidade, gravidade e versões atualizadas do Android (quando aplicável).

As vulnerabilidades corrigidas em 01/03/2019 foram agrupadas em estrutura, mídia e sistema. O grau de gravidade das vulnerabilidades encontradas é determinado pelo impacto sobre a confidencialidade, integridade e disponibilidade da informação. A vulnerabilidade mais grave na seção de estrutura pode permitir que um aplicativo malicioso local execute um código arbitrário dentro de um contexto de processo privilegiado. A seguir, na Figura 12, estão representados os detalhes das vulnerabilidades de estrutura. Foram classificadas como EoP as vulnerabilidades de elevação de privilégio e as vulnerabilidades classificadas como identidade se referem à divulgação da informação.

Figura 12 – Vulnerabilidades de estrutura de dispositivos Android, classificadas por tipo, gravidade e versões atualizadas do AOSP (*Android Open Source Project*)

CVE	Tipo	Gravidade	Versões atualizadas do AOSP
CVE-2018-20346	EoP	Alto	7,0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2019-1985	EoP	Alto	7,0, 7.1.1, 7.1.2, 8.0
CVE-2019-2003	EoP	Alto	7,0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2019-2004	identidade	Alto	7,0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2019-2005	EoP	Moderado	8,0, 8,1 e 9

Fonte: Android Source (2019), online.

A vulnerabilidade mais grave da seção de mídia (representada na Figura 13) pode permitir que um invasor remoto use um arquivo criado para executar um código arbitrário dentro do contexto de um processo privilegiado. As vulnerabilidades classificadas como RCE referem-se à execução remota de código, tendo gravidade crítica devido ao alto risco de exploração das vulnerabilidades.

ISSN: 2595-5942

Revista EduFatec: educação, tecnologia e gestão
V.2 N.1 - janeiro-junho/2019

Figura 13 – Vulnerabilidades de mídia de dispositivos Android, classificadas por tipo, gravidade e versões atualizadas do AOSP (*Android Open Source Project*)

CVE	Tipo	Gravidade	Versões atualizadas do AOSP
CVE-2019-1989	RCE	Crítico	7,0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2019-1990	RCE	Crítico	7,0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2019-2006	EoP	Alto	9
CVE-2019-2007	EoP	Alto	8,1, 9
CVE-2019-2008	EoP	Alto	8,0, 8,1 e 9

Fonte: Android Source (2019), online.

Na seção de sistema, apresentada na Figura 14, a vulnerabilidade mais grave pode permitir que um invasor remoto utilize uma transmissão criada para executar código arbitrário no contexto e um processo privilegiado.

Figura 14 – Vulnerabilidades de sistema de dispositivos Android, classificadas por tipo, gravidade e versões atualizadas do AOSP (*Android Open Source Project*)

CVE	Tipo	Gravidade	Versões atualizadas do AOSP
CVE-2019-2009	RCE	Crítico	7,0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2019-2010	EoP	Alto	7,0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2019-2011	EoP	Alto	8,0, 8,1 e 9
CVE-2019-2012	EoP	Alto	7,0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2019-2013	EoP	Alto	7,0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2019-2014	EoP	Alto	7,0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2019-2015	EoP	Alto	7,0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2019-2016	EoP	Alto	7,0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2019-2017	EoP	Alto	7,0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2019-2018	EoP	Alto	8,1, 9
CVE-2018-9561	identidade	Alto	7,0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2018-9563	identidade	Alto	7,0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2018-9564	identidade	Alto	7,0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2019-2019	identidade	Alto	7,0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2019-2020	identidade	Alto	7,0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2019-2021	identidade	Alto	7,0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2019-2022	identidade	Alto	7,0, 7.1.1, 7.1.2, 8.0, 8.1, 9

Fonte: Android Source (2019), online.

ISSN: 2595-5942

5 Resultados e Discussão

A Figura 6 mostra nitidamente o crescimento do número de dispositivos considerados como inseguros, a diminuição dos talvez seguros e principalmente dos dispositivos considerados seguros**.** Observando-se os extremos outubro de 2011 e abril de 2015 percebe-se que os dispositivos considerados seguros de vulnerabilidades diminuíram de forma intensa, porém se forem comparados os períodos outubro de 2013 e abril de 2015, percebe-se que houve um pequeno crescimento no uso de dispositivos seguros.

Ao observar ambos os gráficos de escore FUM (Figuras 7 e 8), pode-se notar que nenhum fabricante ou dispositivo foi capaz de atingir a pontuação 10 no citado escore, visto que o máximo atingido por fabricante foi a pontuação de 5,76 para dispositivos Nexus e por modelo de dispositivo foi atingido o máximo de 4,74 para o modelo Galaxy Nexus. Os menores escores foram atribuídos ao fabricante Walton, com um escore de 0.27 e ao modelo Symphony W68, com escore 9,91e-05.

Ao analisar o número de vulnerabilidades detectadas por ano em dispositivos Android, representado na Figura 9, percebe-se o aumento considerável, a partir de 2015, tendo seu maior número em 2017. Ao observar os tipos de vulnerabilidades descritos na Figura 10, percebe-se que os três tipos mais encontrados foram, em primeiro lugar *overflow*, em segundo lugar a execução de códigos e em terceiro lugar o ganho de privilégios.

A vulnerabilidade *overflow* consiste na inserção de mais dados do que os campos suportam, ocasionando o estouro do *buffer* de memória e até mesmo o fechamento do aplicativo (MENDES, 2019). A vulnerabilidade de execução de códigos consiste na execução de códigos arbitrários por um determinado servidor remotamente, geralmente mal-intencionado. Por fim, a vulnerabilidade de ganho de privilégios consiste na obtenção de privilégios por um mecanismo malicioso ou atacante, possibilitando o acesso aos recursos e funcionalidades de um dispositivo.

A tabela de tendências de vulnerabilidades ao longo dos anos, apresentada na Figura 11, confirma a vulnerabilidade *overflow* em primeiro lugar, representando 22% do total, seguida pela execução de códigos com 20,7% do total e por fim o ganho de privilégios representando 14,6% do total de vulnerabilidades.

Observando-se os dados apresentados por CVE Details (2019), é possível concluir que houve um crescimento do número de vulnerabilidades em dispositivos

Revista EduFatec: educação, tecnologia e gestão
V.2 N.1 - janeiro-junho/2019

Android ao longo dos anos, tendo seu ponto mais crítico em 2017, no qual as vulnerabilidades de segurança da informação cresceram de forma acelerada.

Apesar da diminuição do número de vulnerabilidades do ano 2017 para 2018, apresentada por CVE Details (2019) na Figura 9, ainda é possível encontrar diversas vulnerabilidades de gravidade alta ou crítica, conforme dados apresentados por Android Source (2019).

Conforme relatado pelos escores FUM, é possível considerar que o aumento do número de vulnerabilidades se deve ao uso de versões desatualizadas de Android, assim como é possível considerar que a diminuição do número de vulnerabilidades pode ter ocorrido devido às novas atualizações do sistema realizadas pelos usuários. Observa-se, por esses fatos, que não depende somente dos fabricantes de dispositivos Android disponibilizarem atualizações frequentes do sistema operacional, a fim de corrigir as vulnerabilidades encontradas anteriormente. É também uma responsabilidade de cada usuário ou empresa de estar atentos às atualizações disponíveis para seus dispositivos Android e ter consciência da importância de realizar tais atualizações de sistema.

A facilidade de instalação de aplicativos duvidosos ou desconhecidos, disponíveis na PlayStore ou em outros mercados de aplicativos para Android, pode contribuir para o surgimento de novas vulnerabilidades, especialmente quando somada à falta de atualização do Android. Esse fato pode tornar preocupante a utilização de dispositivos móveis que utilizam o sistema operacional, tanto de forma profissional quanto pessoal. Muitas pessoas e empresas querem poder adicionar aplicativos e personalizar seus dispositivos móveis, adicionar jogos e diversas ferramentas; contudo, isso pode aumentar a probabilidade de que se instalem através desses aplicativos novas vulnerabilidades que possam tornar suas informações vulneráveis a ataques e ameaças de mecanismos mal-intencionados, visto que uma parte dos aplicativos disponíveis para *download*, especialmente de forma gratuita, são de procedência desconhecida.

É necessário que os fabricantes de dispositivos Android disponibilizem com frequência atualizações de sistema com correções das vulnerabilidades encontradas anteriormente, porém não é suficiente para que os usuários destes dispositivos estejam completamente seguros. Para garantir a segurança de suas informações, é preciso que também os usuários dos dispositivos estejam cientes da importância de realizar as devidas atualizações de sistema, sempre que disponíveis, sabendo que

ISSN: 2595-5942

Revista EduFatec: educação, tecnologia e gestão
V.2 N.1 - janeiro-junho/2019

estas contêm possíveis correções a vulnerabilidades encontradas em versões anteriores do sistema. A prudência ao instalar aplicativos duvidosos ou desconhecidos em seus dispositivos é também uma aliada à segurança das informações de cada usuário, pois, ainda que muitos aplicativos pareçam inofensivos, podem trazer consigo riscos à segurança de suas informações. Por fim, podem partir também da própria PlayStore, ou de outros mercados de aplicativos para Android, mensagens de alerta para os riscos que a instalação de aplicativos de procedência desconhecida podem oferecer ao dispositivo em que são instalados. Dessa forma, alertados dos riscos no momento que acessam as plataformas para realizar o *download*, os usuários poderão repensar se podem confiar a segurança de suas informações aos aplicativos que deseja instalar.

Considerações finais

O objetivo do presente estudo foi analisar as vulnerabilidades de segurança da informação encontradas em dispositivos Android ao longo dos últimos dez anos. Conforme apresentado na primeira seção, a segurança das informações de um indivíduo ou de uma empresa tem sido ameaçada à medida em que seus dados e informações se tornam expostos a mecanismos ou indivíduos mal-intencionados, que se utilizam das vulnerabilidades do sistema operacional para obter acesso ou privilégios sobre esses dados e informações.

A informação é um bem de valor pessoal e profissional que deve ser protegido, visando sempre proteger os pilares da segurança da informação - confidencialidade, integridade e disponibilidade. As vulnerabilidades de segurança da informação surgem quando são ameaçados os pilares da segurança.

No presente estudo, foram consultadas algumas bases de dados *online* a fim de identificar a quantidade, tipo e incidência das vulnerabilidades encontradas. O grande desafio foi encontrar fontes confiáveis, com dados concretos, que auxiliassem na pesquisa. O passo seguinte foi analisar os dados encontrados nessas fontes, gerar gráficos com os dados obtidos e tirar conclusões a respeito desses dados.

Pôde-se concluir, através da pesquisa realizada, que os dispositivos móveis executando o sistema operacional Android em versões desatualizadas se tornam mais susceptíveis a diversas vulnerabilidades de segurança da informação do que

ISSN: 2595-5942

Revista EduFatec: educação, tecnologia e gestão
V.2 N.1 - janeiro-junho/2019

dispositivos que utilizam versões atualizadas do Android. As atualizações de sistema contêm correções de vulnerabilidades encontradas anteriormente e, portanto, devem ser lançadas com frequência regular pelos fabricantes de dispositivos móveis. Outro fator identificado como causador do aumento do número de vulnerabilidades em dispositivos Android é a instalação de aplicativos duvidosos ou desconhecidos, muitas vezes mal-intencionados.

A partir deste artigo poderão ser traçadas métricas e planos para diminuição das vulnerabilidades de segurança encontradas em dispositivos Android, assim como maneiras de conscientizar os usuários destes dispositivos a tratarem com mais prudência a segurança de suas próprias informações.

Agradecimentos

Agradeço a Deus, meu melhor mestre e melhor amigo, que a todo tempo me conduz e fortalece em meu caminho acadêmico e em minha vida. Pude encontrar n'Ele a luz e a força para dar cada passo. Aos meus pais e meu irmão, que me incentivaram e me acalmaram quando o desespero veio, assim como a vontade de desistir. Agradeço ao meu noivo, que acreditou em mim, me impulsionou a me dedicar a esse trabalho e teve paciência quando eu mesma não tive. Ao meu orientador, que de forma paciente me conduziu e norteou, certamente eu não teria conseguido finalizar este trabalho sem o seu auxílio e seu conhecimento. Agradeço aos meus professores e a toda a Fatec Franca, que ao longo dos anos contribuíram ricamente para o meu crescimento e amadurecimento não apenas profissional, mas também pessoal. Aos meus colegas de sala, meu agradecimento por estarmos juntos ao longo desses anos, nos ajudarmos em meio às dificuldades e partilharmos experiências. Aos meus amigos, meu agradecimento pelo companheirismo, apoio e por tornarem minha jornada mais alegre e leve.

Referências

ABNT [ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS] - NBR ISO/IEC 27002:2013. **Tecnologia da Informação - Código de prática para a gestão da Segurança da Informação**. Rio de Janeiro, 2013.

ISSN: 2595-5942

AGRAWAL, A. **Manifest Security. Android Application Security Series**. Disponivel em: <https://manifestsecurity.com/android-application-security-part-2/>. Acesso em: 28 mar. 2019.

ALMEIDA, Josiane. **Análise da segurança e de ferramentas na plataforma Android.** Passo Fundo: Instituto Federal Sul-Rio-Grandense, 2013. Disponível em: <https://painel.passofundo.ifsul.edu.br/uploads/arq/20160330212016137870 2704.pdf >. Acesso em: 22 fev. 2019.

AMARAL, Gustavo; SILVA, Rodrigo; ROTONDO, Gustavo; AMARAL, Érico. **Um estudo sobre vulnerabilidades do Android:** ferramentas e soluções para o usuário**.** Universidade Federal do Pampa e Instituto Federal Sul-Rio-Grandense, 2017. Disponível em:<http://periodicos.unesc.net/sulcomp/article/view/3144/2874>. Acesso em: 22 fev. 2019.

ANDROID SOURCE. **ANDROID SECURITY BULLETIN – March 2019**. Disponível em: <https://source.android.com/security/bulletin/2019-03-01>. Acesso em: 01 abr. 2019.

ANDROID VULNERABILITIES. Universidade de Cambridge – Laboratório de Computação. Disponível em: <http://www.androidvulnerabilities.org/index.html>. Acesso em: 22 mar. 2019.

CERT.br [CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL]. Segurança em Dispositivos Móveis - **Cartilha de Segurança para Internet.** CERT.br, 2017. Disponível em: <https://cartilha.cert.br/dispositivos-moveis/>. Acesso em: 23 fev. 2019.

CONTEÚDO EDITORIAL. **Security Report**. Disponível em: <http://www.securityreport.com.br/destaques/vulnerabilidades-batem-recorde-historico-em-2017/#.XLExI5hKjIU> Acesso em: 12 abr. 2019.

CVE DETAILS. Disponível em: <https://www.cvedetails.com>. Acesso em: 22 mar. 2019.

EBSERH, Hospitais Universitários Federais. **Política de Segurança da Informação e Comunicações (PoSIC)**. Disponível em: <http://www2.ebserh.gov.br/documents/695105/1744025/20170222_PoSIC_minuta_7fev2017_rev+%28004%29.pdf/d05a334b-c46f-41db-8b0e-8411796b1aaa>. Acesso em: 16 abr. 2019.

FONTES, Edison Luiz Gonçalves. **Segurança da Informação.** São Paulo: Saraiva, 2003.

GFI LANGUARD. **Gfi Software Ltd**. Disponível em: <https://manuals.gfi.com/pt-br/languard/content/acm/topics/appendix/common_vulnerabilities_and_exposures__cve_.htm> Acesso em: 01 abr. 2019.

LEITE, Alexandre Canosa; REIS, Helena Macedo. **Comparativo entre sistemas operacionais móveis.** Taquaritinga: Fatec Taquaritinga, 2017. Disponível em:

<http://simtec.fatectq.edu.br/index.php/simtec/article/view/253/236>. Acesso em: 01 abr. 2019.

LEPESQUEUR, Alexandre Mendes Alvim; OLIVEIRA, Italo Diego Rodrigues. **Pentest, Análise e Mitigação de Vulnerabilidades**. Brasília: Universidade de Brasília, 2006. Disponível em: <http://bdm.unb.br/bitstream/10483/13510/1/2012_AlexandreMendesAlvimLepesqueur_ItaloDiegoRodriguesOliveira.pdf>. Acesso em: 23 fev. 2019.

MARCIANO, João Luiz Pereira. **Segurança da informação - uma abordagem social**. Brasília, 2006. CID/FACE-UnB. Disponível em: <http://repositorio.unb.br/bitstream/10482/1943/1/Jo%C3%A3o%20Luiz%20Pereira%20Marciano.pdf>. Acesso em: 21 mar. 2019.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

MENDES, Dimas Albuquerque. **Análise de Vulnerabilidades em aplicações Android com o uso de ferramentas de Teste de Intrusão e a Metodologia OWASP**. Recife: Universidade Federal de Pernambuco, 2017. Disponível em: <http://www.cin.ufpe.br/~tg/2017-2/dam4-tg.pdf>. Acesso em: 23 fev. 2019.