Vulnerabilidade	CWE	OWASP	Quantidade	Aplicação
				Aegis
Missing registerReceiver() exported flag	925	M1	8	AmazeFileManager
Permission name does not follow recommended convention	1099	M1	1	
Cipher.getInstance with ECB	327	M5	2	OmniNotes
Exported service does not require permission	926	M1	1	RetroMusicPlayer
		M2	1	
Implicit intent matches an internal non-exported component	927	M1	7	Wikipedia
		M6	7	
Missing data extraction rules	477	M1	1	

Vulnerabilidade	CWE	OWASP	Quantidade	Aplicação
The initialization vector (IV) is not properly generated	329	M5	1	Aegis
The cipher is susceptible to padding oracle attacks	696	M5	3	
The cipher does not provide data integrity	353	M5	3	
Hard coded password found	259	M9	1	
This random generator (java.util.Random) is predictable	330	M5	1	
The cipher does not provide data integrity	353	M5	1	AmazeFileManager
Hard coded cryptographic key found	321	M9	1	
This use of org/slf4j/Logger.debug(Ljava/lang/String;)V might be used to include CRLF characters into log messages	117,93	M7	4	
Unencrypted server socket (instead of SSLServerSocket)	319	M5	4	
Files could be saved to external storage	312	M2	10	
This API MD5 (MDX) is not a recommended cryptographic hash function	327	M5	2	
Leading zeros are omitted in the concatenation increasing collision potential	704	M7	2	
Possible information exposure through an error message	209,211	M7	1	
The initialization vector (IV) is not properly generated	329	M5	1	
This usage of java/lang/ProcessBuilder. ([Ljava/lang/String;)V can be vulnerable to Command Injection	78	M1	1	
Files could be saved to external storage	312	M2	8	OmniNotes
This web server request could be used by an attacker to expose internal services and filesystem.	73, 918	M3	1	RetroMusicPlayer
				Wikipedia

Vulnerabilidade	CWE	OWASP	Quantidade	Aplicação
Application Data can be Backed up [android:allowBackup=true]	530	M1	1	Aegis
Hidden elements in view can be used to hide data from user. But this data can be leaked	919	M1	5	
The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	649	M5	3	
App creates temp file. Sensitive information should never be written into a temp file.	276	M2	5	
SHA-1 is a weak hash known to have hash collisions.	327	M5	1	
Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	312	M9	2	
The App uses an insecure Random Number Generator.	330	M5	1	
Application Data can be Backed up [android:allowBackup] flag is missing.	530	M1	1	AmazeFileManager
MD5 is a weak hash known to have hash collisions.	327	M5	2	
Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	312	M9	8	
App can read/write to External Storage. Any App can read data written to External Storage.	276	M2	13	
Application Data can be Backed up [android:allowBackup=true]	530	M1	1	OmniNotes
Weak Encryption algorithm used	327	M5	2	
App can read/write to External Storage. Any App can read data written to External Storage.	276	M2	9	
MD5 is a weak hash known to have hash collisions.	327	M5	1	
Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	312	M9	3	
Application Data can be Backed up [android:allowBackup] flag is missing.	530	M1	1	RetroMusicPlayer
Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	312	M9	2	
Application Data can be Backed up [android:allowBackup=true]	530	M1	1	Wikipedia
Remote WebView debugging is enabled.	919	M1	5	
Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	312	M9	2	

Vulnerabilidade	CWE	OWASP	Quantidade	Aplicação
Implement permissions on this exported component.	926	M1	1	Aegis
		M2	1	
Use another cipher mode or disable padding	327	M5	3	
Implement permissions on this exported component.	926	M1	1	AmazeFileManager
		M2	1	
Use a dynamically-generated, random IV	329	M5	1	
Use a dynamically-generated initialization vector (IV) to avoid IV-key pair reuse	323	M5	3	
Use a secure padding scheme	327	M5	2	
Make sure this SSH private key gets revoked, changed, and removed from the code	798, 259	M9	4	
Implement permissions on this exported component.	926	M1	1	OmniNotes
		M2	1	
Change this code to not perform arbitrary intent redirection	20	M1	1	
Use a strong cipher algorithm	327	M5	2	
Use secure mode and padding scheme	327	M5	2	
Implement permissions on this exported component.	926	M1	2	RetroMusicPlayer
		M2	2	
				Wikipedia

	Quantidade	Repetições	Total
M1	40	0	40
M2	51	0	51
M3	1	0	1
M4	0	0	0
M5	41	8	33
M6	7	0	7
M7	7	0	7
M8	0	0	0
M9	23	0	23
M10	0	0	0

	Sonar	MobSF	FindSecBugs	Android Lint
Uso indevido da plataforma (M1)	6	15	1	18
Armazenamento Inseguro de Dados (M2)	5	27	18	1
Comunicação Insegura (M3)	0	0	1	0
Autenticação Insegura (M4)	0	0	0	0
Criptografia Insuficiente (M5)	13	10	16	2
Autorização Insegura (M6)	0	0	0	7
Qualidade do Código do Cliente (M7)	0	0	7	0
Adulteração de Código (M8)	0	0	0	0
Engenharia Reversa (M9)	4	17	2	0
Funcionalidade Irrelevante (M10)	0	0	0	0