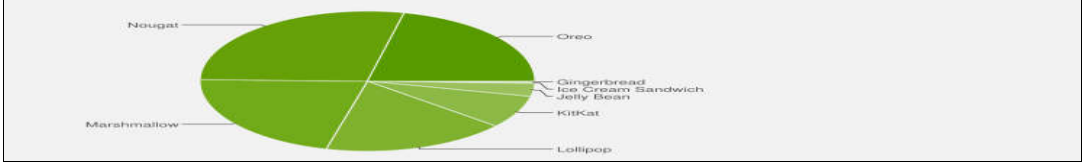
Гавриш О.С. – старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ОСОБЛИВОСТІ БЕЗПЕЧНОГО ВИКОРИСТАННЯ СУЧАСНИХ СМАРТФОНІВ

Як відомо, операційні системи розробляються людьми. У мобільній платформі Google на сьогоднішній день виявлено безліч помилок, деякі з цих помилок являють собою повноцінні уразливості і можуть використовуватися як для несанкціонованого доступу до файлової системи смартфона, так і для поширення шкідливого ПЗ [1].

Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	0.2%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	0.3%
4.1.x	Jelly Bean	16	1.1%
4.2.x		17	1.5%
4.3		18	0.4%
4.4	KitKat	19	7.6%
5.0	Lollipop	21	3.5%
5.1		22	14.4%
6.0	Marshmallow	23	21.3%
7.0	Nougat	24	18.1%
7.1		25	10.1%
8.0	Oreo	26	14.0%
8.1		27	7.5%



Якщо вірити офіційній статистиці Google, на сьогоднішній день серед версій Android найбільш поширена Nougat - редакція мобільної платформи за номером 7.0 і 7.1 встановлена в сукупності на 28,2% пристроїв. Другу позицію впевнено займає Android 8.0 і 8.1 Oreo з показником 21,5%. На третьому місці закріпилася шоста версія Marshmallow - вона працює на 21,3% девайсів. Android 5.0 і 5.1 Lollipop встановлені сумарно на 17,9% пристроїв, а замикає групу лідерів Android 4.4 KitKat з показником 7,6% користувачів.

Згідно з інформацією з сайту cvedetails.com [2], на сьогоднішній день в Android налічується 2146 вразливостей, при цьому число виявлених багів початок експоненціально зростати приблизно з 2014 року.

Не так просто оцінити, скільки з перерахованих пристроїв вчасно отримали оновлення безпеки, які виправили вразливості, але це явно далеко не всі з них. Мало того: не всі вразливості взагалі виявляються закритими, тим більше в старих версіях, офіційна підтримка яких припинена. Проблему посилюють виробники пристроїв, які часто не поспішають випускати оновлення.

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of 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
% Of All		13.7	20.7	22.0	6.1	0.2	0.0	0.1	0.0	5.7	14.1	14.6	0.0	0.0	

Найперша вразливість Android.

Найперша вразливість Android була виявлена ще в жовтні 2008 року в прошивці комунікатора HTC T-Mobile G1. Під час перегляду веб-сторінок з певним вмістом помилка в ПО дозволяла виконати шкідливий код, що відслідковує використання клавіатури гаджета. Теоретично таким чином можна було реалізувати кейлоггер, який фіксує натискання кнопок, і збирати інформацію, що вводиться користувачем при веб-серфінгу інформацію. Ця вразливість була небезпечною тільки для однієї-єдиної моделі комунікатора, але саме її наявність наочно показало: Android - не так безпечна і захищена система, як вважалося раніше.

З ростом популярності операційної системи ентузіасти і дослідники відшукували всі нові і нові помилки в різних її версіях. Безумовно, в рамках однієї статті ми не зможемо охопити всі дві тисячі з гаком вразливостей, виявлених за весь час існування Android. Тому зосередимося тільки на найцікавіших і небезпечних з них, причому - тільки в актуальних на даний момент версіях Android (тих, що зараз ще можуть зустрітися в житті).

Самим «ненадійним» виявилося четверте покоління Android, починаючи з версії 4.4 KitKat. З нього, мабуть, і почнемо наш огляд вразливостей, виявлених в різний час в цій платформі.

BlueBorne CVE: CVE-2017-1000251, CVE-2017-1000250, CVE-2017-0781, CVE-2017-0782, CVE-2017-0785 і CVE-2017-0783.

Уразливі версії Android: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0

Для експлуатації потрібно: атакуючий повинен знаходитися на відстані не більше десяти метрів від уразливого пристрою, а на уразливому пристрої потрібно включити Bluetooth.

Можливий результат: виконання довільного коду з привілеями ядра системи, витік даних. Це не окрема вразливість, а цілий набір помилок в стеці Bluetooth сучасних операційних систем, серед яких значиться і Android. Сер-

йозні помилки містяться в коді системної функції l2cap_parse_conf_rsp ядра Linux, причому їх можна виявити у всіх версіях ядра, починаючи з 3.3. Якщо в системі включена захист від переповнення стека CONFIG_CC_STACKPROTECTOR, їх використання призводить до виникнення критичної помилки в роботі ядра.

Уразливість CVE-2017-1000251 виявлена в модулі ядра під назвою L2CAP, який відповідає за роботу стека протоколу Bluetooth. Ще одна уразливість в стеці цього протоколу отримала позначення CVE-2017-0783. Якщо на атакуємому смартфоні включена підсистема Bluetooth, з її допомогою можна віддалено передати на нього спеціальним чином сформовані пакети інформації. Такі пакети можуть містити шкідливий код, який виконається в Android з привілеями ядра системи. При цьому для реалізації атаки не буде потрібно попередньо сполучати пристрої або включати на них режим виявлення. Досить, щоб атакуючий знаходився на відстані не більше десяти метрів від уразливого пристрою.

Оскільки взаємодіють з протоколом Bluetooth компоненти ОС за замовчуванням мають високі системні привілеї, експлуатація цих вразливостей теоретично дозволяє отримати повний контроль над атакуємим смартфоном і планшетом, включаючи доступ до Вашого пристрою, підключенням мереж і файлової системи. Також за допомогою BlueBorne технічно можна реалізовувати атаки типу man-in-the-middle.

До BlueBorne також відносять вразливість CVE-2017-1000250 в стеці BlueZ Linux протоколу Service Discovery Protocol (SDP). Експлуатація уразливості CVE-2017-1000250 може привести до витоку даних. Вразливості CVE-2017-0781, CVE-2017-0782 і CVE-2017-0785 відносяться до самої ОС Android, при цьому за допомогою перших двох шкідливий додаток може отримати в системі привілеї ядра, а остання дозволяє реалізувати витік даних.

Для усунення вразливостей BlueBorne 9 вересня 2017 року компанія Google випустила оновлення безпеки.

Використані джерела:

1. Самые опасные уязвимости старых версий Android. [Електронний ресурс]. - Режим доступу: https://xakep.ru/2019/02/07/forgotten-android/
2. Vulnerability in the kernel code of the Android operating. [Електронний ресурс]. - Режим доступу: systemhttps://www.cvedetails.com/