https://doi.org/10.53656/math2023-1-7-tot

Overview
Обзор

КЪМ ВЪПРОСА ЗА ПУБЛИЧНО ДОСТЪПНИ НАЦИОНАЛНИ БАЗИ ОТ ДАННИ, СЪДЪРЖАЩИ ОПИСАНИЯ НА УЯЗВИМОСТИ ЗА ОПЕРАЦИОННИ СИСТЕМИ ЗА МОБИЛНИ УСТРОЙСТВА

Стоян Мечев
Висше военноморско училище „Н. Й. Вапцаров“ – Варна

Резюме. В статията се цели да се изследват публично-достъпни бази от данни с уязвимости и техните системи за оценка на тежестта на щетите, които може да нанесе зловреден софтуер, предназначен за мобилни устройства, работещи под операционната система Android или iOS. Втората цел на изследването е да се оценят възможностите за откриване на уязвимости, свързани с конкретна версия на мобилна операционна система. Използвани методи: сравнителен анализ и обобщение. Въз основа на резултатите от прилагането на сравнителния анализ се установява кои от националните бази данни имат по-добри възможности за филтриране на данните и получаване на адекватни резултати при търсене на уязвимости за мобилни устройства.

Ключови думи: Android; iOS; база от данни с уязвимости

1. Въведение

В един съвременен мобилен телефон има възможност за плащания онлайн, двуфакторно удостоверяване при парични преводи, получаване и изпращане на електронна поща, проследяване на местоположението на устройството, записване на видео- и звукови файлове, заснемане на фотографии. Тази голяма функционалност предоставя възможност за много злоупотреби.

По данни на сайта CVE details за последните три календарни години са открити 2329 уязвимости за различни версии на операционната система Android, а за 2023 година вече има открити 27 уязвимости (CVE Details 2023a). Уязвимостите за различни версии на iOS, открити за същия период, са 621 (CVE Details 2023b).

Ето защо точното идентифициране на уязвимостите в мобилните операционни системи (МОС) и тяхното откриване в База от данни с уязвимости (БДУ) е от голямо значение за практиката.

Настоящото изследване може да бъде от полза за специалисти по киберсигурност, разработчици на софтуер за Android и iOS, изследователи в областта на сигурността на мобилни операционни системи и обикновени потребители на мобилни устройства.

2. Актуално състояние на проблема

При проучването на публикациите по темата са изследвани научни статии и доклади, индексирани в Scopus и Web of Science за периода 2017 – 2022 година съгласно препоръките на Jennex (Jennex 2015). Използваните ключови думи са: Android, iOS, vulnerability, vulnerabilities, database. Определянето на изследвания период е базирано на пазарните дялове на различните версии на МОС и е детайлно обосновано в раздел 3 – „Ограничения на изследването".

За първи път през изследвания период NVD се почва от Umasankar като източник на информация за уязвимости за Android (Umasankar 2017).

Tiwari и Velayutham посочват NVD и CVE като основни източници на информация за уязвимости за Android. Разработват приложение, което автоматично да извлича описания на уязвимости от NVD, и споменават за трудности при извличане на детайлната информация относно конкретни уязвимости (Tiwari, Velayutham 2019).

Уязвимостите на Android за периода 2008 – 2017 г. са задълбочено изследвани и класифицирани чрез проучване на CVE (CVE 2022), NVD (NVD 2022) и официалните бюлетини за сигурност на Google. В изследването се споменава, че има уязвимости в огледалната БДУ на NVD – CVE details, които са неправилно класифицирани (Mazuera-Rozo et al. 2019). Подобна констатация е едно от основанията, за да се задълбочи изследването на възможностите на БДУ за коректно извличане на информация относно уязвимости за МОС.

Националните БДУ, NVD, CNVD, CNNVD, JVNDB, наред с други публично достъпни БДУ, са изследвани относно техните възможности за предоставяне на конкретна информация за уязвимости за IoT устройства (Rytel et al. 2020).

И последно, NVD, CNVD, CNNVD са изследвани относно информацията, която предоставят (Forain et al. 2022), но не се разглеждат възможностите за филтриране и извличане на информация за група уязвимости по определен признак, например версия на МОС.

Прави впечатление фактът, че за изследвания период не се откриват публикации по темата на български език или от регион България, индексирани в Scopus или Web of Science.

Следователно може да се твърди, че по посочените БДУ е направен опит за комплексно изследване, но в крайна сметка – с пропуски по отношение на филтрирането на данни за уязвимости за МОС. И това е основанието за настоящото изследване.

3. Ограничения на изследването

Изследвани Бази данни с уязвимости

Дори и беглият поглед върху разнообразието на БДУ за МОС подсказва, че те са десетки или стотици и очевидно се различават по своята достъпност, ефективност и степен на пълнота.

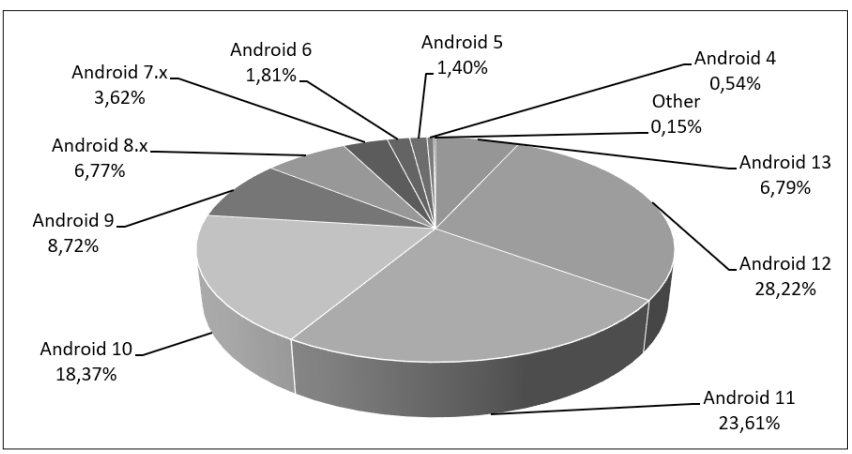
В изследването са включени националните БДУ на държавите с най-голям National Cyber Power Index (NCPI), или на български – Национален индекс за киберсила, за 2020 г. според доклада на Belfer Center for Science and International Affairs Harvard Kennedy School (Voo et al. 2020). Също така е проучено наличието на БДУ на ниво Европейски съюз и на национално ниво, за България.

Изследвани мобилни операционни системи

Изследването на всички МОС е нецелесъобразно, тъй като по данни на *Statcounter GlobalStats* (STATCOUNTER 2023a), в края на 2022 г. пазарните дялове на ОС Android и iOS са били съответно 72,37% и 26,98%, или общо 99,35% от мобилните устройства на пазара са използвали една от двете операционни системи. Пазарният дял на всички останали МОС е под 1% и те би следвало да се изключат от изследването, което в случая е направено.

Изследвани версии на ОС Android

Като се отчете хронологията на внедряване на различните версии на ОС Android (Raphael 2022) и пазарните им дялове в края на 2022 г. (фиг. 1), може да се направи заключението, че изследването на уязвимости за версии, по-ранни от Android 5.0 Lollipop, всъщност не са продуктивни за конкретизираната цел на изследването, тъй като общият пазарен дял на всички по-ранни версии е под 2%.

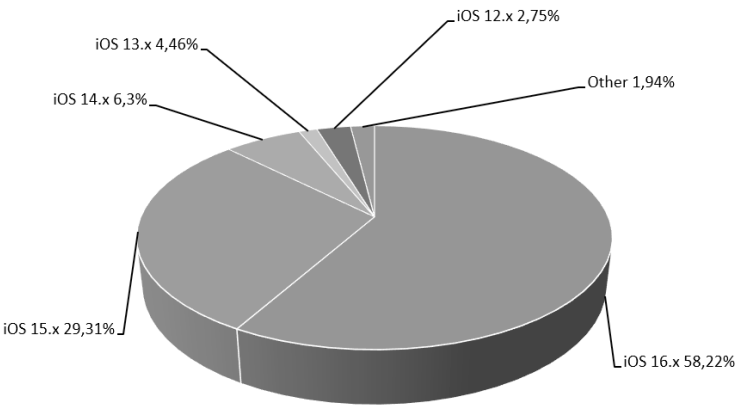


Фигура 1. Пазарни дялове на ОС Android в края на 2022 г. (STATCOUNTER 2023b)

Забележка. Данните са групирани по основни версии на Android OS

Изследвани версии на iOS

След прилагане на същите ограничения, а именно хронологията на внедряване на iOS (Moreau 2021) и пазарния дял (фиг. 2), може да се направи заключението, че не е целесъобразно да се изследват версии на iOS, по-ранни от 12.0.



Фигура 2. Пазарни дялове на iOS в края на 2022 г.(STATCOUNTER 2023c)
Забележка. Данните са групирани по основни версии на iOS

Критерии за оценка

Те са свързани с възможностите за търсене на уязвимости за конкретна версия на МОС.

Критерий 1. Възможности на филтъра.

Критерий 2. Релевантност на откритата информация.

Изложение

Въз основа на резултатите от извършеното проучване по така зададените критерии и ограничения на разкритите информационни ресурси е съставена таблица 1.

Таблица 1. БДУ, подредени по NCPI

1	2	3	4	5	6	7
САЩ	1	NVD	3	CVE	CVSS	182974
КНР	2	CNNVD	1	CNNVD	Собствена и CVSS	194735
КНР	2	CNVD	4	CNVD	Собствена и CVSS	178134
Русия	4	БДУБИ	5	BDU	CVSS	41919
Япония	9	JVN iPedia	2	JVNDB	CVSS	146748
Япония	9	JVN	0	JVN, JVNVU	CVSS	n/a

Забележки:

– Обозначения: 1 – Държава; 2 – NCPI; 3 – Име на БДУ; 4 – Оценка на възможностите за търсене на уязвимости; 5 – Конвенция за именуване на уязвимостите; 6 – Методика за оценка на уязвимостите; 7 – Общ брой записи към датата на проучването.

– Таблицата е съставена по данни, представени по-надолу в изложението.

– В хода на изследването не бяха открити публично достъпни БДУ за МОС на Великобритания (класирана на 3-то място от NCPI), Нидерландия (5-о място), Франция (6-о място), Германия (7-о място), Канада (8-о място) и Австралия (10-о място). БДУ на Европейския съюз и България не са включени в класацията на NCPI.

4. Бази данни с уязвимости (БДУ)

База данни на САЩ

Официалното название на базата е National Vulnerability Database (NVD) (NVD, 2022), което може да се преведе като „Национална база данни за уязвимости“. NVD се поддържа от Националния институт за стандарти и технологии (NIST) към Министерството на търговията на САЩ и работи в тясна връзка с програмата CVE (Common Vulnerabilities and Exposures). Базата данни CVE е изключена от таблицата с базите данни, тъй като, макар и финансирана от правителството на САЩ, се управлява от корпорация MITRE, а не от държавна структура. Освен това е по-скоро глобална, отколкото национална база данни.

NVD има за задача да анализира всяка уязвимост, след като ѝ бъде присвоен уникален идентификатор (CVE ID), и да я класифицира по следните критерии: CWE, CVSS v2.0, CVSS v3.1 и CPE (NVD 2022).

CVE ID е уникален буквено-цифров идентификатор, зададен от програмата CVE. Всеки идентификатор препраща към конкретна уязвимост. CVE ID позволява на множество страни да обсъждат, споделят и съпоставят информация за конкретна уязвимост, знаейки, че се отнасят за едно и също нещо (Mitre 2022).

В основата си Common Weakness Enumeration (CWE) е списък с различни видове софтуерни и хардуерни слабости, като в списъка са включени конкретни и кратки дефиниции за всеки често срещан тип слабост (Mitre 2022).

Общата система за оценяване на уязвимостта (Common Vulnerability Scoring System, CVSS) предоставя начин за представяне на основните характеристики на дадена уязвимост и създаване на числена оценка, отразяваща нейната тежест. След това числеият резултат може да бъде преведен в качествено представяне (като ниско, средно, високо и критично), за да помогне на организациите да оценят правилно и да приоритизират процесите си за управление на уязвимости (FIRST 2022). Действащият стандарт за оценка

на CVSS е CVSS 3.1. При него се определят видовете оценки на уязвимости (таблица 2).

Таблица 2. Скала за оценка на тежестта на уязвимост CVSS 3.1 (FIRST, 2022)

Рейтинг (Rating)	CVSS резултат (Score)
Без рейтинг (None)	0.0
Нисък (Low)	0.1 – 3.9
Среден (Medium)	4.0 – 6.9
Висок (High)	7.0 – 8.9
Критичен (Critical)	9.0 – 10.0

В практиката все още се използва и CVSS 2.0, с което могат да се обяснят незадоволителната популяризация на новата система от критерии и консерватизмът на част от администраторите, които я използват. От друга страна, ако съдим по прилагането на CVSS 2.0 и CVSS 3.1, то следва да направим заключението, че това са добре работещи инструменти, към които правят референции националните бази и на други държави.

Бази данни на КНР

В Китай се поддържат две национални бази от данни с уязвимости – CNNVD и CNVD.

Първата база данни е Китайската национална база данни за уязвимости на информационната сигурност (China National Vulnerability Database of Information Security – CNNVD). Достъпна е само на китайски език. Анализ на уязвимостите и оценка на риска се прави от Китайския център за оценка на информационната сигурност (China Information Security Evaluation Center – CNITSEC) (CNITSEC 2022). В описанията на уязвимостите се използват референции към CVE и CVSS.

Скалата за оценка на уязвимостите на CNNVD е подобна на CVSS 3.1 (таблица 3).

Таблица 3. Таблица за оценка на тежестта на уязвимост (CNNVD 2022)

Ниво на уязвимост	Оценка
Суперкритично (super critical)	9.0 – 10
Висок риск (high risk)	7.0 – 8.9
Среден риск (medium risk)	4.0 – 6.9
Нисък риск (low risk)	0 – 3.9

Забележка. Местата на колоните и градацията на оценките са разменени с цел по-добро съпоставяне с БДУ на САЩ.

Втората БДУ е Китайската национална база данни с уязвимости (China National Vulnerability Database – CNVD). CNVD се поддържа от Националния координационен център за работа с компютърни мрежи в извънредни ситуации (CNCERT). В създаването на CNVD участват национални държавни ведомства, важни потребители на информационни системи, оператори, големи доставчици на средства за сигурност, доставчици на софтуерно осигуряване, научноизследователски институции и публични потребители на интернет (CNVD 2022). В CNVD се публикуват както конкретни уязвимости, така и седмични и месечни бюлетини с обобщена информация. Особеност на китайските бази данни с уязвимости е, че използват цветна кодировка за степените на опасност.

База данни на РФ

Официалното название на базата е Банк данных угроз безопасности информации (БДУБИ), което може да се преведе като „Банка от данни със заплахи за информационната сигурност“. Поддържа се от Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю, или Държавен научноизследователски изпитателен институт по проблемите на техническата защита на информацията към Федералната служба по технически и експортен контрол.

БДУБИ съдържа информация за основните заплахи и уязвимости за информационната сигурност, предимно специфични за държавните информационни системи и автоматизираните системи за управление на производствените и технологичните процеси на критични съоръжения (БДУБИ 2022).

На този етап БДУБИ все още прави референции към NVD и в една или друга степен може да се смята за неин аналог.

Бази данни с уязвимости на Япония

В Япония се поддържат две БДУ – JVN и JVN iPedia.

Официалното англоезично название на първата БДУ е Japan Vulnerability Notes (JVN) (JVN 2022), което може да се преведе като „Японски записи за уязвимости“. Това е портален сайт за информация за уязвимости, предназначен да помогне за гарантиране на интернет сигурността чрез предоставяне на информация за уязвимости и техните решения за софтуерни продукти, използвани в Япония. JVN се управлява съвместно от Координационния център JPCERT и Агенцията за насърчаване на информационните технологии (IPA).

Официалното англоезично название на втората БДУ е JVN iPedia. По същество JVN iPedia се разглежда като разширение на JVN. В допълнение към информацията за противодействие на уязвимостите, публикувана на JVN, това е база данни с информация за противодействие на уязвимости, която се публикува ежедневно както в Япония, така и в чужбина (JVN iPedia 2022). Особеност на JVN iPedia е, че макар самият сайт да има интерфейс на ан-

глийски език, само малка част от описанията на уязвимостите са преведени от японски.

Официално и двете японски БДУ са съвместими с глобалната БДУ CVE, препратките към която са разположени на заглавните им страници.

5. Източници, изключени от изследването

В хода на изследването беше установено, че във Великобритания, Нидерландия, Франция, Германия, Канада и Австралия, а така също и в Европейския съюз функционират организации, които предоставят информация за уязвимости на МОС. Но информацията, предоставяна от съответните организации, или не е публично достъпна, или не е реализирана като БДУ. По тази причина тези източници не са предмет на настоящото изследване (UK NCSC 2022), (NL NCSC 2022), (CERT-FR 2022), (BDI 2022), (CCTX 2022), (AUSCERT 2022), (CERT-EU 2022).

В България функционира Националната лаборатория по компютърна вирусология (НЛКВ) към БАН (БАН 2022). Тя не поддържа собствена база от данни за злонамерен софтуер и злонамерени атаки (Polimirova 2022).

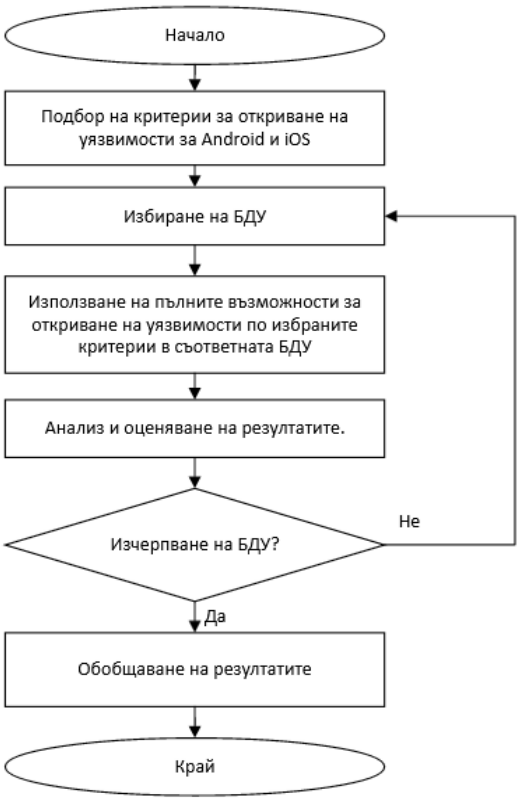
Другата българска организация, свързана с проблемите на киберсигурността, е Националният екип за реагиране при инциденти в компютърната сигурност, или CERT България (CERT Bulgaria 2022). На сайта на CERT България се публикува информация за уязвимости, която е на английски език и няма никаква възможност за търсене и филтриране на информацията. Предоставяната информация се отнася само за 2022 г. и не е реализирана като БДУ. Ето защо и двете български структури са неподходящи източници на информация по приетите ограничения за целите на изследването.

Обсъждане и резултати

Всяка от анализираните БДУ има вградени възможности за търсене на уязвимости със задаване на допълнителни условия за филтриране на резултатите. Създава се впечатлението, че откриването на уязвимости за конкретна версия на МОС е лесна за решаване задача. Опитът показва, че това всъщност не е така. Оказва се, че в резултатите от търсенето освен уязвимости, свързани с конкретна версия на МОС, се появява и информация, която в една или друга степен не е релевантна спрямо зададените условия.

Използвани са вградените възможности за търсене и филтриране на всяка една от анализираните БДУ. Направени са опити да се открият уязвимости за конкретни версии на Android и iOS, отговарящи на ограниченията на изследването.

Обследването на всяка БДУ преминава през следните стъпки, отразени на фигура 3.



Фигура 3. Блок-схема на експеримента

В резултат на извършеното обследване на информационните ресурси са очертани следните възможности за филтриране на информацията при изследваните БДУ. Те са представени в таблица 4.

Таблица 4. Възможности за филтриране на информацията в БДУ

Възможности на филтъра	Оценка	БДУ с такива възможности
Няма възможност за търсене. Информацията е подредена в раздели, по хронологичен ред на публикациите.	0	JVN
Търсене по идентификатор на уязвимост (CNVD или CVE), ниво на риск, период на публикуване на уязвимостта и период на обновление на информацията за уязвимостта. Няма възможност за търсене по операционна система или производител на хардуер.	1	CNNVD

Търсене по ключова дума, разработчик (производител), продукт, дата на публикуване, дата на последно обновление, CVSSv3, CVSSv2 и CWE.	2	JVN iPedia
Търсене по ключова дума, CVE номер на уязвимост, продукт, дата на публикуване, дата на последно обновление, CVSSv3, CVSSv2, CWE, CPE. CPE по същество позволява задаване на разработчик на продукта, наименование и версия на продукта.	3	NVD
Търсене по ключова дума, CNDV номер на уязвимост, дата на публикуване, наличие на референтна информация, разработчик (производител), продукт, версия на продукта, причина за уязвимостта, заплахи, причинени от уязвимостта, тежест на заплахата, разположение на експлойта спрямо атакуваното устройство.	4	CNVD
Търсене по ключова дума, производител на програмното осигуряване, тип на програмното осигуряване, в което е открита уязвимостта, наименование на програмното осигуряване, апаратна платформа, версия на програмното осигуряване, няколко подверсии на основната версия на МОС, статус на уязвимостта. Допълнителни параметри – времеви период, в който е установена уязвимостта, година на добавяне на уязвимостта, клас на уязвимостта, ниво на опасност, базов CVSS вектор, идентификатор на типа на грешката по CWE, идентификатор на грешката в друга БДУ, наличие на експлойт, способ за експлоатиране на уязвимостта, способ за отстраняване на уязвимостта, операционна система.	5	БДУБИ

Забележка

1. Присвоените стойности за оценка са въз основа на експертния опит на автора.

2. Експлойтът представлява код, който се възползва от уязвимост на софтуера или пропуск в сигурността (TREND MICRO, 2022).

3. Всяка неанглоезична БДУ при автоматичен превод на английски език загубва от своята функционалност.

4. На JVN се присъжда оценка 0, защото няма възможност за търсене.

Конкретните резултати от обследването очертават следните особености на анализираните БДУ.

CNNVD предоставя възможности за търсене само по идентификатор на уязвимост (CNNVD или CVE), което не позволява да се търсят група уязвимости, свързани с конкретна версия на МОС.

При **JVN iPedia** и **NVD** се наблюдават фалшиви позитивни резултати при търсене по ключова дума (False-positive result). Например тази слабост се проследява при Android 5.0 в случая: https://web.archive.org/web/20210620220718/https://jvndb.jvn.jp/en/contents/2020/JVNDB-2020-000081.html

Частен случай на посочения недостатък се установява при **NVD**. При него при задаване на условието „точно съвпадение“ по отношение на ключовата дума тя се открива дори когато е част от по-дълъг текстов низ. Пример: при търсене на **iOS 15.0** се откриват уязвимости, свързани с **iOS 15.0.1**, **iOS 15.0.2** и т.н.

NVD дава много добри резултати за откриване на конкретна версия за Android с помощта на CPE. За съжаление, CPE не може да се използва при търсене на уязвимости за iOS.

Това следва да се счита за значим недостатък. По данни на Apple (APPLE 2023) iOS 16 се поддържа от 23 различни модела на iPhone, най-старият от които е от 2016 година (Jones 2023). Това може да доведе до подвеждащи резултати относно уязвимостите за конкретно устройство. Например при търсене по CPE за модел на iPhone от 2019 г. ще бъдат открити уязвимости за устройството, а не уязвимости за iOS 16, която е реализирана през 2022 г.

Филтърът на **CNVD** дава възможност за избор на разработчик, но при избиране на фирмите, разработващи Android и Apple iOS, се наблюдават повторения на стойностите, макар че се избират от падащ списък. Например Google може да се открие три пъти, което подвежда потребителя.

Въпреки че БДУБИ има най-малък брой записи (табл. 1), то от изложеното в таблица 4 става ясно, че тя има значителни предимства по отношение на филтрирането пред останалите БДУ, с които се извършва сравнението.

Препоръки

Да се разширят възможностите на NVD за филтриране на данни, като се добави възможност за филтриране по операционна система.

7. Изводи

1. Установяват се две основни тенденции относно предоставянето на информация за уязвимости за МОС: от една страна, поддръжка на публична база, а от друга – публично-частни партньорства без предоставяне на публична информация за уязвимостите.
2. Търсенето на уязвимости по МОС понякога дава нерелевантни резултати. Установяването на тяхната честота може да бъде предмет на отделно изследване.
3. Към 2022 г. наложеният стандарт за оценка на тежестта на дадена уязвимост е CVSS (табл. 1).
4. Нито една база не позволява извличане на реални статистически данни за брой на уязвимости за МОС.

Благодарности и финансиране

Това изследване е подкрепено от Министерство на образованието и науката по Националната програма "Млади учени и постдокторанти-2".

Acknowledgments & Funding

This research is supported by the Bulgarian Ministry of Education and Science under the National Program "Young Scientists and Postdoctoral Students - 2".

REFERENCES

APPLE, 2023. iPhone models compatible with iOS 16 – Apple Support. [online]. 30 January 2023. [Accessed 11 February 2023]. Available from: https://web.archive.org/web/20230130120403/https://support.apple.com/guide/iphone/supported-models-iphe3fa5df43/ios

AUSCERT, 2022. Australia's LEADING cyber emergency response team. *AUSCERT.* [Online] 2022-09-19. [Cited: 2022-09-19]. Available from: https://web.archive.org/web/20220919000852/https://auscert.org.au/.

BDI, 2022. UP KRITIS. *Bundesamt für Sicherheit in der Informationstechnik.* [Online] 2022-08-11. [Cited: 2022-09-25]. Available from: https://web.archive.org/web/20220811085322/https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/UP-KRITIS/up-kritis_node.html.

BDUBI, 2022. Bank dannykh ugroz bezopasnosti informatsii. Bank dannykh ugroz bezopasnosti informatsii. [Online] 2022-10-06. [Cited: 2022-10-06]. Available from: https://web.archive.org/web/20221006232715/https://bdu.fstec.ru/.

CCTX, 2022. ABOUT CCTX. CCTX. [Online] 2022-03-27. [Cited: 2022-09-20]. Available from: https://web.archive.org/web/20220327174736/https://cctx.ca/about-cctx/.

CERT BULGARIA, 2022. CERT BULGARIA. *BULGARIAN COMPUTER SECURITY INCIDENTS RESPONSE TEAM.* [Online] 2022-07-26. [Cited: 2022-08-25]. Available from: https://web.archive.org/web/20220726101323/https://www.govcert.bg/BG/Pages/default.aspx.

CERT-EU, 2022. Publications. *CERT-EU.* [Online] 2022-08-15. [Cited: 2022-09-01]. Available from: https://web.archive.org/web/20220815090149/https://cert.europa.eu/publications.

CERT-FR, 2022. CERT-FR. *CERT-FR.* [Online] 2022-10-02. [Cited: 2022-10-02]. Available from: https://web.archive.org/web/20221002202558/https://www.cert.ssi.gouv.fr/.

CNITSEC, 2022. China Information Security Evaluation Center. *China Information Security Evaluation Center.* [Online] 2022-05-01. [Cited: 2022-

08-10]. Available from: https://web.archive.org/web/20220501130155/http://www.cnnvd.org.cn/web/xxk/gyCnnvdJs.tag.

CNNVD, 2022. CNNVD Vulnerability Classification Specification. *CNNVD.* [Online] 2022-05-01. [Cited: 22-08-10]. Available from: https://web.archive.org/web/20220501130153/http://www.cnnvd.org.cn/web/wz/bzxqById.tag?id=2&mkid=2.

CNVD, 2022. Introduction to CNVD. *CNVD.* [Online] 2022-10-14. [Cited: 14 10 2022-10-14]. Available from: https://www.cnvd.org.cn/webinfo/list?type=7.

CURRY, D., 2022. Android version market share. *Business of Apps.* [Online] 2022-09-16. [Cited: 2022-09-25]. Available from: https://web.archive.org/web/20220916231934/https://www.businessofapps.com/data/android-statistics/.

CVE, 2022. Glossary. *CVE.* [Online] 2022-10-01. [Cited: 2022-10-10]. Available from: https://web.archive.org/web/20221001032257/https://www.cve.org/ResourcesSupport/Glossary?activeTerm=glossaryCVEID.

CVE DETAILS, 2023a. Google Android : CVE security vulnerabilities, versions and detailed reports. [online]. 14 February 2023. [Accessed 15 February 2023]. Available from: https://web.archive.org/web/20230215063933/https://www.cvedetails.com/product/19997/Google-Android.html

CVE DETAILS, 2023b. Apple Iphone Os : CVE security vulnerabilities, versions and detailed reports. [online]. 15 February 2023. [Accessed 15 February 2023]. Available from: https://web.archive.org/web/20230215065258/https://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49

FIRST, 2022. Common Vulnerability Scoring System SIG. *Forum of Incident Response and Security Teams.* [Online] 2022-08-31. [Cited: 2022-09-12]. Available from: https://web.archive.org/web/20220831232945/https://www.first.org/cvss/.

FIRST, 2022. Common Vulnerability Scoring System v3.1: Specification Document. *Forum of Incident Response and Security Teams.* [Online] 2022-07-19. [Cited: 2022-08-21]. Available from: https://web.archive.org/web/20220719233119/https://www.first.org/cvss/v3.1/specification-document.

FORAIN, I., ALBUQUERQUE, R., JÚNIOR, R. T., 2022. *Towards System Security: What a Comparison of National Vulnerability Databases Reveals.* Madrid. ISBN: 978-989-33-3436-2.

JENNEX, Murray E., 2015. Literature reviews and the review process: An editor-in-chiefs perspective. *Communications of the Association for Information Systems*, vol. 36, 39–146. DOI 10.17705/1CAIS.03608.

JONES, Matthew, 2023. iPhone History: Every Generation in Timeline Order 2007-2023. [online]. 12 January 2023. [Accessed 11 February 2023]. Available from: https://web.archive.org/web/20230112023356/https://historycooperative.org/the-history-of-the-iphone/

JVN iPedia, 2022. JVN iPedia. *JVN iPedia.* [Online] 2022-10-01 [Cited: 2022-10-01]. Available from: https://web.archive.org/web/20221001042457/https://jvndb.jvn.jp/en/.

JVN, 2022. Japan Vulnerability Notes. *Japan Vulnerability Notes.* [Online] 2022-09-03. [Cited: 2022-09-20]. Available from: https://web.archive.org/web/20220903085032/http://jvn.jp/.

MAZUERA-ROZO, A., et al., 2019. The Android OS stack and its vulnerabilities: an empirical study. *Springer Science+Business Media*, LLC.

MITRE, 2022. Common Weakness Enumeration. *Common Weakness Enumeration.* [Online] 2022-09-14. [Cited: 2022-09-20]. Available from: https://web.archive.org/web/20220914235250/https://cwe.mitre.org/data/index.html.

MOREAU, S., 2021. The evolution of iOS. *Computerworld.* [Online] 2021-06-18. [Cited: 2022-09-16.]. Available from: https://web.archive.org/web/20220412035433/https://www.computerworld.com/article/2975868/ the-evolution-of-ios.html#.

NL NCSC, 2022. Become an NCSC partner and receive relevant information. *NATIONAAL CYBER SECURITY CENTRUM.* [Online] 2022-04-21. [Cited: 2022-09-07]. Available from: https://web.archive.org/web/20220421172916/https://english.ncsc.nl/get-to-work/become-a-partner.

NLCV, 2022. About. National Laboratory of Computer Virology of BAS. [Online] 2022-09-30. [Cited: 2022-10-02]. Available from: https://web.archive.org/web/20220930110714/https://www.nlcv.bas.bg/bg/aboutUs-104.

NVD, 2022. CVEs and the NVD Process. *NATIONAL VULNERABILITY DATABASE.* [Online] 2022-05-14. [Cited: 2022-09-01]. Available from: https://web.archive.org/web/20220514082423/https://nvd.nist.gov/general/cve-process.

NVD, 2022. CVE FAQs. *National Vulnerability Database.* [Online] 2022-10-18. [Cited: 2022-10-18]. Available from: https://web.archive.org/web/20221018115922/https://nvd.nist.gov/general/FAQ-Sections/CVE-FAQs.

NVD, 2022. NATIONAL VULNERABILITY DATABASE. *NATIONAL VULNERABILITY DATABASE.* [Online] 2022-08-04. [Cited: 2022-08-10]. Available from: https://web.archive.org/web/20220804163449/https://nvd.nist.gov/.

POLIMIROVA, D. 2022-07-12. Nalichie na natsionalna baza danni s uyazvimosti. Email [personal communication].

RAPHAEL, JR., 2022. Android versions: A living history from 1.0 to 13. *Computerworld* [Online] 2022-08-23 r. [Cited: 2022-09-10]. Available from: https://www.computerworld.com/article/3235946/android-versions-a-living-history-from-1-0-to-today.html

RYTEL, M., FELKNER, A., & JANISZEWSKI, M., 2020. Towards a Safer Internet of Things – A Survey of IoT Vulnerability Data Sources. *Sensors*. 20, 5969. doi:10.3390/s20215969.

STATCOUNTER GLOBAL STATS, 2022. iOS Version Market Share Worldwide. *Statcounter GlobalStats.* [Online] 2022-01-31. [Cited: 2022-09-20]. Available from: https://web.archive.org/web/20220131220904/https://gs.statcounter.com/ios-version-market-share/all/worldwide/2021.

STATCOUNTER, 2023a. Mobile Operating System Market Share Worldwide | Statcounter Global Stats. [online]. 23 February 2023. [Accessed 13 February 2023]. Available from: https://web.archive.org/web/20230207073026/https://gs.statcounter.com/os-market-share/mobile/worldwide/

STATCOUNTER, 2023b. Android Version Market Share Worldwide | Statcounter Global Stats. [online]. 13 February 2023. [Accessed 13 February 2023]. Available from: https://gs.statcounter.com/android-version-market-share/all/worldwide/2022

STATCOUNTER, 2023c. iOS Version Market Share Worldwide | Statcounter Global Stats. [online]. 13 February 2023. [Accessed 13 February 2023]. Available from: https://gs.statcounter.com/ios-version-market-share/all/worldwide/2022

STATS, STATCOUNTER GLOBAL, 2022. Mobile Operating System Market Share Worldwide - December 2021. *Statcounter Global Stats.* [Online] 2022-09-01. [Cited: 2022-09-01]. Available from: https://web.archive.org/web/20220110031504/https://gs.statcounter.com/os-market-share/mobile/worldwide#.

TIWARI, Pradeep Kumar and VELAYUTHAM, T., 2019. Android Vulnerabilities: Taxonomy and nextGen Ecosystem. *2019 IEEE Bombay Section Signature Conference, IBSSC 2019*, vol. 2019January. DOI 10.1109/IBSSC47189.2019.8973083.

TREND MICRO, 2022. exploit. *TREND MICRO.* [Online] 2022-10-17. [Cited: 2022-10-17]. Available from: https://web.archive.org/web/20221017053736/https://www.trendmicro.com/vinfo/us/security/ definition/exploit.

UK NCSC, 2022. CISP - Cyber Security Information Sharing Partnership. *National Cyber Security Centre (UK).* [Online] 2022-09-02. [Cited: 20 09

2022-09-20]. Available from: https://web.archive.org/web/20220902073419/https://www.ncsc.gov.uk/section/keep-up-to-date/cisp.

UMASANKAR, 2017. Analysis of latest vulnerabilities in android. *2017 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2017*, vol. 2017-January, 1236–1241. DOI 10.1109/ICACCI.2017.8126011.

VOO, J., et al., 2020. *National Cyber Power Index 2020.* Cambridge: Belfer Center for Science and International Affairs, 2020.

TO THE ISSUE OF PUBLICLY AVAILABLE NATIONAL DATABASES CONTAINING DESCRIPTIONS OF VULNERABILITIES FOR MOBILE DEVICE OPERATING SYSTEMS

Abstract. The paper aims to examine publicly available vulnerability databases and their systems for assessing the severity of damage that can be caused by malware targeting mobile devices running Android or iOS. The second goal of the study is to evaluate the vulnerability detection capabilities associated with a specific version of a mobile operating system. Methods used: comparative analysis and summary. Based on the results of the application of the comparative analysis, it is established which of the national databases have better capabilities to filter the data and obtain adequate results when searching for vulnerabilities for mobile devices.

Keywords: Android; iOS; vulnerability database

✉ **Stoyan Mechev, PhD student**
Web of Science Researcher ID: AAB-4270-2021
ORCID iD: 0000-0002-0809-8538
Nikola Vaptsarov Naval Academy
73, Vasil Drumev Str.
Varna, Bulgaria
E-mail: st.mechev@naval-acad.bg