Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных машин

Дисциплина: Защита информации в информационных системах

ОТЧЕТ
по практическй работе №1
на тему
Анализ уязвимостей операционных систем семейства Windows

Студент:

Проверил:

МИНСК 2024

1. ЦЕЛЬ РАБОТЫ

Изучение наиболее актуальных обнаруженных уязвимостей в операционных системах семейства Windows с использованием базы данных CVE и других доступных источников.

2. Ответы на практическую часть

1) Рейтинг наиболее распространенных уязвимостей для ОС:

- SQL-инъекции (SQL Injection)
- Переполнение буфера (Buffer Overflow)
- XSS (Cross-Site Scripting)
- Удаленное выполнение кода (Remote Code Execution, RCE)
- Уязвимость повышенной привилегии (Privilege Escalation)
- Уязвимость в криптографических протоколах
- Уязвимости в аутентификации (Authentication Bypass)
- Директории для обхода (Path Traversal)
- CSRF (Cross-Site Request Forgery)
- Уязвимости в сторонних библиотеках

2) Рейтинг наиболее опасных уязвимостей для ОС:

- CVE-2017-0144 (EternalBlue)
- CVE-2019-0708 (BlueKeep)
- CVE-2020-0601 (CurveBall)
- CVE-2018-4878 (Flash Zero-Day)
- CVE-2021-26855 (ProxyLogon)
- CVE-2014-6271 (Shellshock)
- CVE-2014-0160 (Heartbleed)
- CVE-2020-1472 (ZeroLogon)
- CVE-2008-4250 (MS08-067)
- CVE-2021-34527 (PrintNightmare)

3) Общее количество обнаруженных уязвимостей ПО в 2023 году:

По данным Национального института стандартов и технологий США (The National Institute of Standards and Technology, NIST), количество обнаруженных за 2023 год уязвимостей (28 902).

4) 10 основных уязвимостей ОС Windows за весь период наблюдения:

- CVE-2017-0144 (EternalBlue): уязвимость в SMBv1, использованная для распространения WannaCry.
- CVE-2020-0601 (CurveBall): уязвимость в криптографическом алгоритме.
- CVE-2019-0708 (BlueKeep): удаленное выполнение кода через RDP.
- CVE-2012-0158: уязвимость в Microsoft Office, эксплуатируемая через документы Word.
- CVE-2008-4250 (MS08-067): удаленное выполнение кода в службе сетевых ресурсов.
- CVE-2020-1472 (ZeroLogon): уязвимость в протоколе Netlogon.
- CVE-2019-1367: ошибка в Internet Explorer, связанная с обработкой памяти.
- CVE-2015-1635: уязвимость в HTTP.sys, используемая для DDoS-атак.
- CVE-2010-3338: уязвимость в Windows Kernel.
- CVE-2016-0189: уязвимость в JScript, позволяющая выполнение кода.
-

5) Уязвимости ПО на июнь 2013 г.:

- VE-2013-0422 (Java SE Zero-Day)
- CVE-2013-0634 (Flash Player Zero-Day)
- CVE-2013-1493 (Java Applet Exploit)
- CVE-2013-2551 (Internet Explorer Use-After-Free)
- CVE-2013-3918 (Remote Code Execution in Windows)
- CVE-2013-1347 (Internet Explorer Zero-Day)
- CVE-2013-7331 (Windows TCP/IP Stack Vulnerability)
- CVE-2013-2465 (Oracle Java Buffer Overflow)
- CVE-2013-3163 (Windows Kernel Privilege Escalation)
- CVE-2013-3893 (Internet Explorer Memory Corruption)

6) Уязвимости ПО на июнь 2023 г. и тренд:

- CVE-2021-44228 (Log4Shell)
- CVE-2021-34527 (PrintNightmare)
- CVE-2022-22965 (Spring4Shell)
- CVE-2022-3786 (OpenSSL Buffer Overflow)
- CVE-2022-40684 (Fortinet Authentication Bypass)

- CVE-2022-30190 (Follina)
- CVE-2022-34718 (Windows TCP/IP Remote Code Execution)
- CVE-2022-31889 (Zimbra Zero-Day)
- CVE-2023-23397 (Microsoft Outlook Elevation of Privilege)
- CVE-2023-27350 (PaperCut MF/NG Remote Code Execution)

7) Уязвимости в Windows Server 2019:

Windows Server 2019 подвергся большому количеству критических атак, связанных с уязвимостями, что требовало срочных обновлений безопасности. Такие уязвимости, как ZeroLogon и CurveBall, могли нарушить инфраструктуру больших организаций, если они не были устранены. По состоянию на 2023 год, в Windows Server 2019 было зарегистрировано более 200 уязвимостей, включая критические уязвимости.

8) Уязвимости в Windows XP:

Windows XP стала крайне уязвимой после завершения поддержки, и атаки на эту ОС продолжались даже спустя годы, когда пользователи и организации продолжали её использовать без обновлений безопасности. Windows XP стала крайне уязвимой после завершения поддержки, и атаки на эту ОС продолжались даже спустя годы, когда пользователи и организации продолжали её использовать без обновлений безопасности.

9) Уязвимости в Windows 11:

Windows 11, будучи относительно новой ОС, получает регулярные обновления безопасности, и многие из обнаруженных уязвимостей уже устранены патчами. Однако даже учитывая это, на текущий момент было обнаружено более 100 уязвимостей.

10) Описание уязвимостей:

- CVE-2017-1000229: Уязвимость в библиотеке GNU Libgcrypt, позволяющая удаленное выполнение кода.
- CVE-2020-29385: Уязвимость в WebKitGTK, которая позволяет обход механизмов защиты.
- CVE-2020-1179: Уязвимость в Microsoft SharePoint, позволяющая эскалацию привилегий.

- CVE-2021-26855: Уязвимость ProxyLogon в Microsoft Exchange, позволяющая удаленное выполнение кода.
- CVE-2024-45623: Поскольку это уязвимость 2024 года, нужно следить за её появлением в базе CVE.

3. Ответы на контрольные вопросы

1. **Физический: (0, 1)**
   Работа со средой передачи, сигналами и двоичными данными.
   Оборудование: концентратор, повторитель.
2. **Канальный: (кадры)**
   Физическая адресация.
   Оборудование: сетевой мост, коммутатор.
3. **Сетевой: (пакеты)**
   Определение маршрута и логическая адресация
   Оборудование: маршрутизатор, сетевой шлюз.
4. **Транспортный: (сегменты)**
   Прямая связь между конечными пунктами и надёжность.
   Оборудование: хосты, межсетевой экран.
5. **Сеансовый: (работа с сеансами)**
   Управление сеансом связи.
   Оборудование: хосты, межсетевой экран.
6. **Представления: (преобразования данных)**
   Представление и шифрование данных.
   Оборудование: хосты, межсетевой экран.
7. **Прикладной: (запросы)**
   Доступ к сетевым службам
   Оборудование: хосты, межсетевой экран. Более пожробно про каждый уровень

4. ЗАКЛЮЧЕНИЕ

Изученил наиболее актуальные обнаруженные уязвимости в операционных системах семейства Windows с использованием базы данных CVE и других доступных источников.