Уязвимости в OS Windows

Добро пожаловать на презентацию о распространенных уязвимостях в ОС Windows. Мы рассмотрим типы вредоносных программ, риски безопасности, а также лучшие практики и инструменты для обнаружения и устранения уязвимостей.

Выполнили:
Сальников Василий
Писарев Степан

Значимость осведомленности о уязвимостях

Осведомленность о уязвимостях в ОС Windows является критически важной для обеспечения безопасности компьютерных систем. Каждый день в сети появляются новые угрозы, которые могут нанести серьезный ущерб вашей системе и вашей конфиденциальности. ОС Windows является одной из наиболее распространенных операционных систем, что делает ее особенно привлекательной для злоумышленников.

Распространенные уязвимости в ОС Windows

1 **Уязвимость исполнения кода (Code Execution)**

Возникает, когда злоумышленник может запустить свой вредоносный код на уязвимой системе, обходя защитные механизмы. Это может произойти через вредоносные вложения в электронной почте, недостаточно защищенные сетевые сервисы или эксплойты, использующие известные уязвимости.

2 **Уязвимость несанкционированного доступа (Unauthorized Access)**

Эта уязвимость позволяет злоумышленнику получить доступ к данным или ресурсам без необходимых разрешений или аутентификации. Например, слабые пароли, уязвимости в механизмах аутентификации или недостаточные правила доступа могут привести к несанкционированному доступу к системе.

3 **Уязвимость отказа в обслуживании (Denial of Service - DoS)**

Возникает, когда злоумышленник создает условия, при которых ресурсы системы исчерпываются, что приводит к недоступности системы для легитимных пользователей. Это может быть вызвано эксплуатацией слабостей в сетевых протоколах, программном обеспечении или

4 **Уязвимость повышения привилегий (Privilege Escalation)**

Позволяет злоумышленнику получить более высокий уровень доступа к системе, чем должен быть у него по умолчанию. Это может произойти через использование слабых настроек безопасности, ошибок в программном обеспечении или недостаточно строгие политики

Риски безопасности, связанные с устаревшей ОС Windows

1. Уязвимости без обновлений

Устаревшая ОС Windows не получает важные обновления безопасности, что увеличивает риск возникновения уязвимостей.

2. Отсутствие поддержки

Майкрософт прекращает поддержку старых версий ОС Windows, не обновляя и не обеспечивая их безопасность.

3. Совместимость с новыми ПО

Устаревшие версии ОС Windows могут быть несовместимы с новыми программами, что ограничивает функциональность и безопасность.

Лучшие практики защиты ОС Windows

1

1. Обновление системы

Регулярно обновляйте ОС Windows, чтобы исправлять известные уязвимости.

2. Использование антивирусного ПО

Это поможет защитить вашу операционную систему от вирусов, троянов, шпионского ПО и других вредоносных программ. Регулярное обновление баз данных антивируса обеспечивает

3. Осторожность в интернете

Будьте осторожны при скачивании и открытии файлов из ненадежных источников.

Инструменты и методы для обнаружения и устранения уязвимостей в ОС Windows

Vulnerability Scanners

Инструменты для поиска уязвимостей в системе и определения необходимых патчей.

Intrusion Detection Systems

Системы, которые мониторят сеть на предмет вторжений и осуществляют реакцию при обнаружении.

Security Patches

Официальные обновления, выпущенные разработчиками программного обеспечения для исправления уязвимостей и ошибок.

Примеры реальных уязвимостей в ОС Windows

Уязвимость SMBGhost (CVE-2020-0796)

- Эта уязвимость затрагивает протокол SMBv3 и позволяет злоумышленнику удаленно выполнить произвольный код на компьютере с уязвимой версией Windows.
- Атакующий может получить полный контроль над системой, если она уязвима.
- Microsoft выпустила патч для исправления этой уязвимости в марте 2020 года.

BlueKeep (CVE-2019-0708)

- Это уязвимость в сервисе удаленного рабочего стола (RDP), которая позволяет удаленному злоумышленнику выполнить произвольный код на компьютере под управлением уязвимой версии Windows.
- Атакующий может распространить вредоносное ПО в сети без взаимодействия с пользователем.
- Microsoft выпустила исправление для этой уязвимости в мае 2019 года.

Уязвимость EternalBlue (CVE-2017-0144)

- Эта уязвимость касается протокола SMBv1 и позволяет удаленному злоумышленнику выполнить произвольный код на компьютере с уязвимой версией Windows.
- Уязвимость была использована в крупных кибератаках, включая атаку WannaCry в 2017 году, что привело к значительным последствиям для организаций и частных лиц по всему миру.
- Microsoft выпустила исправление для этой уязвимости в марте 2017 года.

Заключение и основные выводы

ОС Windows подвержена множеству уязвимостей, которые могут быть использованы злоумышленниками. Чтобы обезопасить свою систему, необходимо следовать лучшим практикам защиты и использовать инструменты для обнаружения и устранения уязвимостей.