Анализ уязвимости и Best Practices

Часть 1: Разбор уязвимости

CVE: CVE-2024-38030

Описание:
Zero-day уязвимость, связанная с утечкой учётных данных New Technology LAN Manager (NTLM) — набора разработанных Microsoft протоколов безопасности, которые используются для аутентификации пользователей и компьютеров в сети. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, проводить спуфинг атаки.

Исследователи обнаружили данную уязвимость в операционной системе Windows, связанную с темами оформления. Она позволяет злоумышленникам удалённо красть учётные данные NTLM. Проблема остаётся актуальной на всех версиях Windows — от 7 до 11.

Эксплуатация NTLM давно используется в Relay-атаках, где хакеры заставляют уязвимые устройства подключаться к подконтрольным серверам, получая доступ к конфиденциальным данным, и в атаках «pass-the-hash», в которых уязвимости используются для получения NTLM-хешей (хешированные пароли) с целевых систем.
Получив хеш, атакующие могут аутентифицироваться как скомпрометированный пользователь, получая доступ к конфиденциальным данным и распространяясь по всей сети. Год назад Microsoft объявила о намерении отказаться от протокола аутентификации NTLM в будущих версиях Windows 11.

Для эксплуатации уязвимости пользователь должен либо скопировать файл темы, например, из электронного письма или чата в папку или на рабочий стол, либо посетить вредоносный сайт, с которого файл автоматически скачивается в папку **Загрузки**

CWE, связанные с уязвимостью:

- CWE-200 — Exposure of Sensitive Information to an Unauthorized Actor (раскрытие конфиденциальной информации неавторизованному субъекту) — это категория уязвимостей, при которой чувствительная информация становится доступной лицам, которым не положено её видеть.

Оценка по CVSS

- **Итоговый балл:** 6,5 (Medium)
  Уязвимость имеет средний уровень серьезности. Она представляет собой умеренную угрозу, может быть использована при определенных условиях или требует некоторых усилий со стороны злоумышленника.

- **Вектор:** `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N`

Разбор метрик

В процессе разбора метрик данной уязвимости, после более детального рассмотрения, у меня не возникло расхождений с оценкой данной уязвимости при подсчете на калькуляторе CVSS 3.

- **AV:N (Network)** — Уязвимость эксплуатируется удалённо.
  Для эксплуатации уязвимости злоумышленнику достаточно отправить потенциальной жертве файл темы Windows и заставить её провести с ним некоторые манипуляции. После этих манипуляций Windows отправляет на удалённые хосты аутентифицированные сетевые запросы с учётными данными NTLN, принадлежащими пользователю.
- **AC:H (Low)** — Специальной подготовки не требуется.
  Для подготвки уязвимости не требуется специальной сложной подготовки, достаточно разослать спам-письма с соответствующим содержимым.
- **PR:N (None)** — Привилегии не требуются.
  Специальных привелегий не требуется, так как главное действие выполняется пользователем, а уязвимость эксплуатируется удаленно.
- **UI:N (Required)** — Требует выполнения действия со стороны пользователя.
  Чтобы эксплуатировать уязвимость, пользователь должен либо скопировать файл темы, например, из электронного письма или чата в папку или на рабочий стол, либо посетить вредоносный сайт, с которого файл автоматически скачивается в папку „Загрузки“. То есть некоторые действия со стороны потенциальной жертвы всё-таки необходимы
- **S:U (Unchanged)** — Атака не выходит за границы компонента.
- **C:H (High)** — Утечка конфиденциальной информации (NTLM-хэши).
  Данная уязвимость оказывает влияние на конфиденциальность информации. Получив NTLM хеш, атакующие могут аутентифицироваться как скомпрометированный пользователь, получая доступ к конфиденциальным данным и распространяясь по всей сети.
- **I:N (None)** — Целостность не затрагиваются.
- **A:N (None)** — Доступность не затрагиваются.

Описание последствий

Возможные последствия

- Утечка NTLM-хэшей, раскрытие NTLM-учетные данные пользователя, передача их на машину злоумышленника.
- Компрометация доменной учетной записи - получив NTLM хеш, атакующие могут аутентифицироваться как скомпрометированный пользователь.
- Возможность проведения relay-атак и offline-брутфорса.

Варианты эксплуатации

- Отправка email с внешними ссылками (например, изображение из внешнего домена).
- Посещение вредоносного сайта, с которого файл автоматически скачивается в папку „Загрузки“.
- Outlook автоматически делает NTLM-запрос, раскрывая учетные данные.

Злоумышленнику необходимо убедить пользователя загрузить вредоносный файл на уязвимую систему — обычно с помощью заманчивого сообщения по электронной почте или через мессенджер — а затем убедить пользователя каким-то образом взаимодействовать с специально созданным файлом, но не обязательно кликать по нему или открывать его.

Вывод

Рекомендации и патчи

- Установка обновлений безопасности от Microsoft (июль 2024)
- Блокировка использования NTLM-хэшей с помощью групповой политики.

  Примените существующую групповую политику для блокировки хэшей NTLM. При включении этой политики проблема для клиента или сервера, подключающегося к удалённому SMB-ресурсу, может быть устранена.

  Чтобы включить политику, выполните следующее:
  Перейдите в Конфигурация компьютера > Конфигурация Windows > Параметры безопасности > Локальные политики > Параметры безопасности.
  В правой панели дважды щёлкните политику Сетевые параметры безопасности: Ограничить использование NTLM: Исходящий трафик NTLM к удалённым серверам и установите одно из значений, указанных в [документации по политике "Сетевые параметры безопасности: Ограничить использование NTLM: Исходящий трафик NTLM к удалённым серверам"].
- Отключение автоматической загрузки внешних ресурсов в Outlook.
- Инструктаж по информационной безопасности сотрудников организации. Доведение до них информации о том, что даже простое скачивание файлов из сети может нести опасность для конфиденциальности данных их учетных записей.
- Использование SMB Signing и других мер против NTLM Relay.

Почему опасно игнорировать данный тип уязвимости

Несмотря на то, что данная уязвимость имеет лишь средний уровень опасности по оценке CVSS, она довольно легко эксплуатируется и не требует специальных знаний и навыков. Для её успешной эксплуатации может быть достаточно средств социальной инженерии, при этом последствия такой

атаки позволяют злоумышленникам получить данные достаточные для аутентификации под учетными данными пользователя.

Все это усугубляется тем, что данная атака не требует непосредственных действий со скачанным файлом. Даже у продвинутого пользователя ПК, не имеющего специальных знаний в области ИБ есть устоявшиеся мнение, что для того, чтобы "вирус проник на компьютер" необходимо его запустить. Это может усыпить блительность рядового пользователя и дать злоумышленнику возможность воспользоваться этим.

Часть 2: Лучшие практики — Безопасная разработка веб-приложений

Best Practices

1. **Валидация и очистка пользовательского ввода** - Не доверяйте данным от клиента.

   Зачем

   Чтобы защититься от XSS, SQL-инъекций, и других атак, использующих недоверенные данные.

   Как

   Используйте серверную валидацию (например, Joi, express-validator).

   Проверяйте типы, длину, допустимые значения. Не полагайтесь на фронтенд.

   OWASP Input Validation

2. **Минимизация прав доступа**

   Зачем

   Чтобы при компрометации пользователь/сервис не получил доступ к лишним ресурсам.

   Как

   - Пользователи, сервисы и БД должны иметь только необходимые привилегии.
   - Принцип наименьших привилегий (Least Privilege).

3. **Хранение паролей с использованием современных алгоритмов**

   Зачем

   Чтобы при утечке базы данных пароли нельзя было восстановить.

   Как

   Использование криптографически стойких алгоритмов шифрования

OWASP Password Storage Cheat Sheet

4. **Повсеместное использование HTTPS**

   Зачем

   Чтобы предотвратить перехват данных (MITM-атаки).

   Как

   - Включить HSTS
   - Запретите использование HTTP
   - Перенаправление HTTP траффика на HTTPS
   - Использование TLS-сертификатов

5. **Защита от CSRF**

   Зачем

   Чтобы злоумышленник не мог выполнять действия от имени пользователя без его ведома.

   Как

   - Добавление CSRF-токенов в формы
   - Проверка форм на сервере

6. **Регулярное обновление зависимостей**

   Зачем

   Чтобы устранить уязвимости в сторонних библиотеках.

   Как

   Автоматизация проверок актуальности зависимостей (`npm audit`, `OWASP Dependency-Check`, `Dependabot`)

7. **Content Security Policy (CSP)**

   Зачем

   Чтобы предотвратить XSS и загрузку вредоносных скриптов.

   Как

   Настроить заголовок Content-Security-Policy, указывая допустимые источники (script-src, style-src, и т. д.).

   OWASP CSP Guide
