УДК 004.056.5

Валентин БЕВЗ

Західноукраїнський національний університет

АНАЛІЗ АКТУАЛЬНИХ ВРАЗЛИВОСТЕЙ MS OFFICE

Вступ. Аналіз актуальних вразливостей MS Office є надзвичайно важливим через широку поширеність цього програмного забезпечення в урядових, корпоративних та освітніх установах. Зловмисники часто використовують уразливості в MS Office як вектор для фішингу, доставки шкідливого коду та ескалації привілеїв. Регулярне дослідження таких вразливостей дозволяє своєчасно виявляти загрози, зменшувати ризики компрометації систем і підвищувати загальний рівень кіберзахисту. Це робить тему особливо актуальною в умовах зростання кількості кібератак на документообіг та офісні середовища.

Мета: виявлення, класифікація та аналіз актуальних вразливостей у програмному середовищі MS Office, а також оцінка їхнього впливу на інформаційну безпеку користувачів. Особлива увага приділяється методам виявлення та усунення цих вразливостей, а також рекомендаціям щодо зменшення ризиків їх експлуатації.

1. Аналіз сучасних загроз офісним застосункам MS Office

Загальну кількість виявлених уразливостей будемо аналізувати за даними бази CVE. Усього за другий квартал 2024 року там було опубліковано інформацію про 8559 уразливостей. Це не остаточна цифра, оскільки часто дані в цій базі оновлюються «заднім числом». Це трохи більше за показники другого кварталу 2023 року: кількість вразливостей, інформація про які стає публічною, продовжує зростати. Із загальної кількості уразливостей 332 є критичними.

За неповною статистикою за перше півріччя 2024 року можна зробити висновок про зниження частки багів, для яких доступний публічний експлойт або Proof of Concept. Зате зросла кількість інцидентів, у яких використовуються вразливі легітимні драйвери для програмного забезпечення.

Найбільш серйозними вразливостями, що найчастіше використовуються зловмисниками для Windows будуть наступні вразливсоті:

– CVE-2018-0802 – вразливість у компоненті Equation Editor пакету Microsoft Office;

– CVE-2017-11882 – ще одна вразливість у Equation Editor, схема зараження якого приведена на рисунку 1.

– CVE-2017-0199 - вразливість у Microsoft Office та WordPad;

– CVE-2021-40444 - вразливість віддаленого виконання коду в компоненті MSHTML.

У другому кварталі 2024 року було відзначено значне зростання атак на користувачів систем на базі Linux з використанням експлойтів для поширених уразливостей. Серед найчастіше експлуатованих багів два (CVE-2022-0847, CVE-2023-2640) відносяться до ядра системи. Ще одна вразливість (CVE-2021-4034) відноситься до утиліти pkexec, що дозволяє виконувати команди від імені іншого користувача.

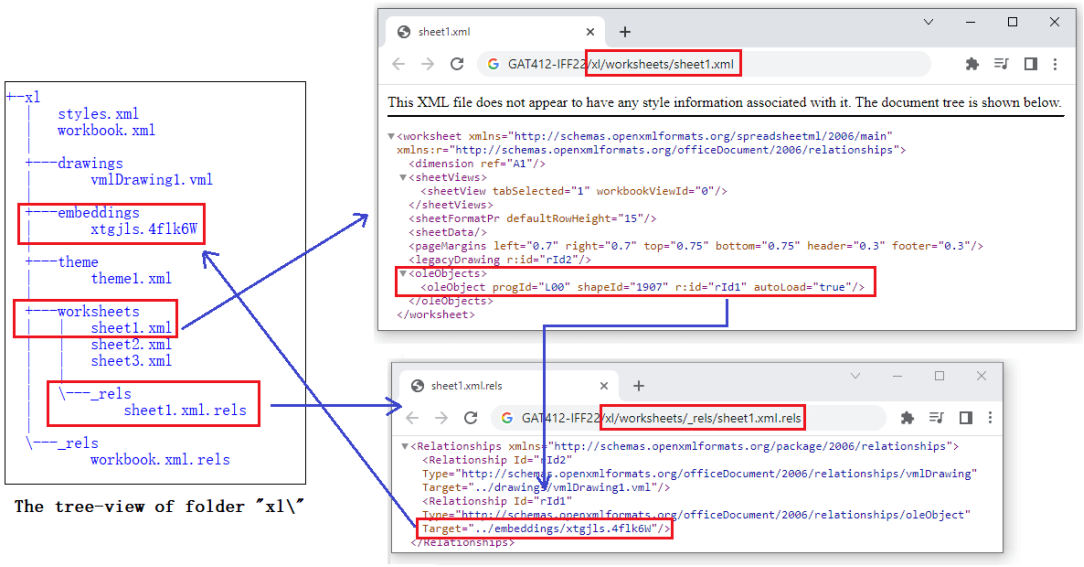

Рисунок 1 - Схема вразливості CVE-2017-11882

Якщо «користувальницьке» шкідливе ПЗ експлуатує одні і ті ж уразливості роками, то в атаках на бізнес частіше застосовуються експлойти до нещодавно виявлених проблем в корпоративному ПЗ. виявленим у 2024 році: CVE-2024-3400 для програмного забезпечення Palo Alto Networks, CVE-2024-20353 для рішень Cisco, CVE-2024-1709 у ПЗ для IT-менеджменту ConnectWise, а також відома вразливість CVE-2024e2 Зловмисники, що атакують компанії, шукають насамперед уразливі точки входу в корпоративну мережу та регулярно оновлюють набір інструментів, що використовуються.

2. Аналіз вразливості CVE-2022-30190

30 травня Microsoft розкрила деталі вразливості нульового дня у всіх версіях локального та хмарного офісного пакету MS Office, також надала рекомендації IT-фахівцям із захисту від експлойту, який доступний у мережі деякий час.

Microsoft зареєструвала цю вразливість під номером CVE-2022-30190. Компанія поки що не випустила проти неї патчі, розробники займаються цим інцидентом.

Ця вразливість зазнає всіх версій Microsoft Office з 2016 по 2021 і Office 365. З її допомогою зловмисник може віддалено запустити довільний код. У мережі вже є кілька підтверджень, що ця вразливість використовувалася під час атак. Експерти навели приклад експлойту для цієї вразливості, коли проаналізували шкідливий документ Word 05-2022-0438.doc, нещодавно завантажений на VirusTotal.

12 квітня дослідник Shadowchasing1 повідомив Microsoft про проблему і надіслав до Microsoft Security Response Center (MSRC) приклад експлойту.

21 квітня MSRC закрила тикет, заявивши, що проблема не пов'язана з безпекою, проігнорувавши, що в експлойті відбувається виконання msdt з відключеними макросами.

У травні Microsoft, ймовірно, намагалася виправити цю вразливість у новій тестовій версії Office 365. Компанія не задокументувала CVE щодо цього

інциденту.

27 травня експерти виявили факти застосування зловмисниками цієї вразливості та знову повідомили у MSRC. Заражений документ використовує функцію віддаленого шаблону Word для вилучення HTML-файлу з віддаленого сервера, який використовує URI схему ms-msdt MSProtocol для завантаження коду та виконання скриптів PowerShell. Microsoft Word виконує код через інструмент підтримки ms-msdt навіть за відключених макросів. Захищений перегляд запускається, але якщо змінити документ на формат RTF, захищений перегляд включається навіть без відкриття документа, наприклад, через вкладку попереднього перегляду у Провіднику. На рисунку 2 приведено фрагмент коду з зараженого документа.

```
$cmd = "c:\windows\system32\cmd.exe";Start-Process $cmd -windowstyle hidden -ArgumentList "/c
taskkill /f /im msdt.exe";Start-Process $cmd -windowstyle hidden -ArgumentList "/c cd C:\users
\public\&&for /r %temp% %i in (05-2022-0438.rar) do copy %i 1.rar /y&&findstr TVNDRgAAAA
1.rar>1.t&&certutil -decode 1.t 1.c &&expand 1.c -F:* .&&rgb.exe";
```

Рисунок 2 - Приклад коду, що виконується при запуску спеціально зараженого документа

У результаті Microsoft погодилася, що вразливість дійсно критична і опублікувала додаткові рекомендації з безпеки клієнтів офісного пакету.

Microsoft рекомендує системним адміністраторам вимкнути протокол MSDT URL за допомогою команди "reg delete HKEY_CLASSES_ROOT\ms-msdt /f", попередньо зробивши резервну копію цього ключа реєстру ("reg export HKEY_CLASSES_ROOT\ms-msdt filename").

Також для блокування використання вразливості можна включити в налаштуваннях Microsoft Defender правило для відображення напрямків атаки BlockOfficeCreateProcessRule, яке забороняє програмам Office створювати дочірні процеси.

Microsoft радить в офісних пакетах не відключати в налаштуваннях захисту параметри за замовчуванням Protected View і Application Guard, які також запобігають можливості використання вразливості нульового дня CVE-2022-30190, але не для всіх версій MS Office.

Microsoft пообіцяла випустити незабаром необхідні оновлення для всіх версія MS Office проти нової вразливості.

Висновок. У результаті проведеного аналізу встановлено, що MS Office залишається одним із найбільш привабливих об'єктів для атак через підтримку макросів, складні формати документів і глибоку інтеграцію з операційною системою. Більшість вразливостей пов'язані з соціальною інженерією та використанням шкідливих вкладень у документах. Регулярне оновлення програмного забезпечення, обмеження прав доступу та використання сучасних засобів захисту дозволяють істотно знизити ризики. Отримані результати можуть бути використані для підвищення кіберстійкості як окремих користувачів, так і організацій.

Перелік використаних джерел.

1. Security Update Guide [Електронний ресурс]. – Режим доступу: https://msrc.microsoft.com/update-guide/vulnerability