**Nguyễn Thành Trung**

**Mssv: 2024802010496  
Trình bày cơ chế, tác động và cách khắc phục của các CVE:**

**CVE-2024-30080 - Lỗ hổng thực thi mã từ xa của Microsoft Message Queuing (MSMQ)**

Là một phần của Microsoft Patch Tuesday tháng 6, Microsoft đã vá một lỗ hổng nghiêm trọng (điểm CVSS 9.8) Message Queuing (MSMQ) CVE-2024-30080.

*Cơ chế, tác động:*

Những kẻ tấn công từ xa, không được xác thực có thể khai thác vấn đề này để thực thi mã tùy ý với các đặc quyền nâng cao của các hệ thống nơi MSMQ được bật. Lỗ hổng có thể lây nhiễm giữa các máy chủ nơi MSMQ bị tắt.

Để khai thác lỗ hổng, kẻ tấn công phải gửi một loạt các gói MSMQ được thiết kế đặc biệt theo trình tự nhanh qua HTTP đến máy chủ MSMQ đến các máy chủ dễ bị tấn công và do đó khai thác lỗ hổng,kẻ tấn công có thể thực thi mã từ xa và chiếm quyền kiểm soát máy chủ chưa được vá. Lỗ hổng được báo cáo ảnh hưởng đến nhiều hệ điều hành Windows bắt đầu từ Windows Server 2008 và Windows 10.

*Cách khắc phục:*

Để xác định xem hệ thống của bạn có dễ bị tấn công hay không, hãy kiểm tra xem tính năng MSMQ HTTP-Support có được bật không và có dịch vụ nào đang chạy có tên là Message Queuing trên máy không.

Nếu *Message Queue Service* không được sử dụng trong Trung tâm dữ liệu Symantec, Quản trị viên DCS có thể tắt dịch vụ này:

Chặn dịch vụ MSMQ chạy bằng Quy tắc tăng cường ứng dụng DCS cho %systemroot%\system32\mqsvc.exe -> Từ chối Sandbox

Nếu cần sử dụng Dịch vụ hàng đợi tin nhắn, Quản trị viên DCS có thể giảm bề mặt tấn công bằng cách thêm quy tắc củng cố Mạng toàn cầu đến để giới hạn các kết nối đến MSMQ trên port: 1801 tới các nguồn đáng tin cậy nội bộ.

Ngoài ra, sandbox bảo mật mặc định cho dịch vụ MSMQ sẽ bảo vệ máy chủ Windows khỏi việc khai thác lỗ hổng này bằng cách chặn việc sử dụng tệp nhị phân LOL cho các hoạt động độc hại, đánh cắp thông tin đăng nhập và cài đặt các công cụ phần mềm độc hại trái phép.

**CVE-2024-30103 - Lỗ hổng thực thi mã từ xa trong Microsoft Outlook**

CVE-2024-30103 là lỗ hổng thực thi mã từ xa ảnh hưởng đến Microsoft Outlook. Lỗ hổng này có mức độ nghiêm trọng cơ bản là CAO với điểm cơ bản là 8,8. Nó yêu cầu đặc quyền thấp và không yêu cầu tương tác của người dùng để khai thác, khiến nó trở thành mối đe dọa đáng kể. Vectơ tấn công là thông qua mạng và nó có tác động lớn đến cả tính toàn vẹn và tính bảo mật.

*Cơ chế:*

CVE-2024-30103 cho phép kẻ tấn công thực thi mã tùy ý trên hệ thống bị ảnh hưởng thông qua nội dung email được thiết kế đặc biệt. Lỗ hổng tồn tại do Microsoft Outlook xử lý không đúng cách các đối tượng trong bộ nhớ, có thể bị khai thác để truy cập và kiểm soát trái phép hệ thống. Lỗ hổng này có điểm cơ sở CVSS v3 là 8,8, cho thấy mức độ nghiêm trọng cao của nó. Phân tích bao gồm điểm tác động là 5,9 và điểm khả năng khai thác là 2,8, phản ánh rủi ro đáng kể mà nó gây ra cho các hệ thống bị ảnh hưởng

*Tác động:*

Mối quan tâm chính đối với CVE-2024-30103 là khả năng thực thi mã từ xa. Nếu bị khai thác, kẻ tấn công có thể thực thi mã độc trong bối cảnh đặc quyền của người dùng trên hệ thống bị xâm phạm. Điều này có thể dẫn đến vi phạm dữ liệu, thao túng hệ thống và khai thác thêm mạng. Với việc sử dụng rộng rãi Microsoft Outlook trong môi trường doanh nghiệp và cá nhân, tác động tiềm ẩn là đáng kể.

*Cách khắc phục:*

Để giảm thiểu rủi ro liên quan đến CVE-2024-30103, người dùng và quản trị viên cần áp dụng các bản vá bảo mật mới nhất do Microsoft cung cấp. Cập nhật phần mềm là một trong những cách hiệu quả nhất để bảo vệ chống lại các lỗ hổng. Microsoft đã phát hành các bản cập nhật giải quyết vấn đề cụ thể này và chúng tôi khuyến nghị nên ưu tiên triển khai các bản vá này cho tất cả các hệ thống bị ảnh hưởng.

Ngoài ra, người dùng nên thận trọng khi xử lý email từ các nguồn không xác định hoặc không đáng tin cậy. Việc triển khai các biện pháp bảo mật tốt nhất, chẳng hạn như vô hiệu hóa macro và đảm bảo lọc email mạnh mẽ, có thể làm giảm thêm nguy cơ bị khai thác.

**CVE-2024-30078 - Lỗ hổng thực thi mã từ xa trong Windows Wifi-Driver**

CVE-2024-30078 là lỗ hổng bảo mật nghiêm trọng ảnh hưởng đến Trình điều khiển Wi-Fi của Windows. Nó cho phép thực thi mã từ xa, nghĩa là kẻ tấn công ở gần thiết bị mục tiêu có thể gửi các gói Wi-Fi được thiết kế đặc biệt để khai thác lỗ hổng. Nếu khai thác thành công, điều này có thể cho phép kẻ tấn công thực thi mã tùy ý trên hệ thống mục tiêu, có khả năng dẫn đến xâm phạm toàn bộ hệ thống. Lỗ hổng được đánh giá với điểm CVSS là 8,8, cho thấy mức độ nghiêm trọng cao.

*Cơ chế:*  
Kẻ tấn công không cần truy cập vật lý vào thiết bị nhưng phải ở trong phạm vi Wi-Fi. Lỗ hổng phát sinh từ việc xác thực đầu vào không đúng trong trình điều khiển Wi-Fi, có thể bị thao túng để thực thi mã độc hại.

*Tác động:*  
Lỗ hổng này ảnh hưởng đến tất cả các phiên bản Windows phổ biến, bao gồm Windows 10, Windows 11 và nhiều phiên bản Windows Server khác nhau từ năm 2008 trở đi. Microsoft coi việc khai thác lỗ hổng này là "ít có khả năng xảy ra", nhưng do tác động lớn và dễ khai thác nên đây là rủi ro bảo mật đáng kể.

*Cách khắc phục:*  
Bản vá bảo mật giải quyết CVE-2024-30078 đã được Microsoft phát hành như một phần của bản cập nhật Patch Tuesday tháng 6 năm 2024. Bản cập nhật KB này khắc phục lỗ hổng bằng cách sửa quy trình xác thực đầu vào trong trình điều khiển Wi-Fi, do đó ngăn chặn vectơ khai thác mà kẻ tấn công sử dụng để truy cập trái phép và thực thi mã từ xa (BleepingComputer).

Kiểm tra bản cập nhật KB: Đảm bảo rằng bản cập nhật KB cụ thể có địa chỉ CVE-2024-30078 được cài đặt trên hệ thống của bạn.

Cài đặt bản cập nhật: Nếu bản cập nhật chưa được cài đặt, hãy sử dụng Windows Update hoặc tải xuống và cài đặt bản vá theo cách thủ công từ Danh mục Microsoft Update.

Xác minh cài đặt: Sau khi cài đặt, hãy xác minh rằng hệ thống được bảo vệ bằng cách kiểm tra danh sách các bản cập nhật đã cài đặt.

**Lỗ hổng thực thi mã từ xa trong Microsoft Office**

**CVE-2024-30101**

CVE-2024-30101 là lỗ hổng thực thi mã từ xa của Microsoft Office, ảnh hưởng đến sản phẩm CMlzl. Lỗ hổng có mức độ nghiêm trọng cơ bản là CAO và điểm cơ bản là 7,5, gây ra mối nguy hiểm tiềm ẩn cho các tổ chức. Điểm khả năng khai thác là 1,6, cho thấy lỗ hổng có thể bị khai thác tương đối dễ dàng. Các đặc quyền cần thiết để khai thác là KHÔNG CÓ, nhưng cần có tương tác của người dùng. Vectơ tấn công là thông qua mạng. Tác động đến tính toàn vẹn và tính bảo mật đều là CAO. Để khắc phục lỗ hổng này, các tổ chức nên áp dụng các bản vá hoặc cập nhật bảo mật cần thiết do Microsoft cung cấp để đảm bảo các sản phẩm Office của họ được an toàn.

**CVE-2024-30102**

CVE-2024-30102 là lỗ hổng thực thi mã từ xa của Microsoft Office ảnh hưởng đến sản phẩm wZun0e. Lỗ hổng có mức độ nghiêm trọng cơ bản là CAO, với điểm cơ bản là 7,3 trên 10. Nó yêu cầu các đặc quyền và tương tác của người dùng thấp để khai thác và vectơ tấn công là cục bộ. Tác động bao gồm các tác động cao về tính toàn vẹn và tính bảo mật. Lỗ hổng có thể được khắc phục bằng cách áp dụng các bản vá hoặc bản cập nhật bảo mật cần thiết do Microsoft cung cấp. Nếu không được vá, lỗ hổng này gây ra mối nguy hiểm đáng kể cho các tổ chức vì nó cho phép thực thi mã từ xa, có khả năng dẫn đến truy cập trái phép, vi phạm dữ liệu và khai thác thêm hệ thống hoặc mạng bị ảnh hưởng.

**CVE-2024-30104**

CVE-2024-30104 là lỗ hổng thực thi mã từ xa trong Microsoft Office ảnh hưởng đến sản phẩm CMlzl. Lỗ hổng có mức độ nghiêm trọng cơ bản là CAO với điểm cơ bản là 7,8, cho thấy mức độ nguy hiểm tiềm tàng của nó đối với các tổ chức. Lỗ hổng này yêu cầu tương tác của người dùng và có vectơ tấn công là LOCAL, khiến kẻ tấn công phải có quyền truy cập vào hệ thống mục tiêu. Tác động của lỗ hổng bao gồm tác động cao đến tính toàn vẹn và tính bảo mật, với tác động đến tính khả dụng cũng được xác định là cao. Chi tiết về biện pháp khắc phục không được cung cấp trong thông tin được cung cấp và hiện tại không có phân tích nào cho lỗ hổng này.

**Lỗ hổng thực thi mã từ xa trong Microsoft SharePoint CVE-2024-30100**

CVE-2024-30100 là lỗ hổng trong Microsoft SharePoint Server cho phép thực thi mã từ xa. Sản phẩm bị ảnh hưởng là Jjxt4Z. Để khắc phục lỗ hổng, các tổ chức sử dụng sản phẩm bị ảnh hưởng nên áp dụng các bản vá hoặc bản cập nhật bảo mật cần thiết do Microsoft cung cấp. Mối nguy hiểm tiềm ẩn đối với một tổ chức là rất cao, vì lỗ hổng này có thể bị kẻ tấn công khai thác mà không cần bất kỳ đặc quyền nào và cần có sự tương tác của người dùng. Nó có mức độ nghiêm trọng cơ bản là CAO và điểm cơ bản là 7,8 theo CVSS phiên bản 3.1, cho thấy mối đe dọa đáng kể đối với tính bảo mật, tính toàn vẹn và tính khả dụng của dữ liệu.