

**ỦY BAN NHÂN DÂN
HUYỆN THAN UYÊN**

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc**

Số: /UBND - PVH

Than Uyên, ngày tháng 4 năm 2023

V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 4/2023

Kính gửi:

- Các cơ quan, ban, ngành, đoàn thể huyện;
- Ủy ban nhân dân các xã, thị trấn.

Ngày 11/4/2023, Microsoft đã phát hành danh sách bản vá tháng 04 với 97 lỗ hổng bảo mật trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý các lỗ hổng bảo mật có mức ảnh hưởng cao và nghiêm trọng sau:

- Lỗ hổng bảo mật **CVE-2023-28252** trong Windows Common Log File System Driver cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế.

- Lỗ hổng bảo mật **CVE-2023-21554** trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa.

- 03 lỗ hổng bảo mật CVE-2023-23384, CVE-2023-23375, CVE-2023-28304 trong Microsoft SQL Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2013-3900** xác thực chữ ký WinVerifyTrust cho phép đối tượng tấn công có thể thêm nội dung vào phần chữ ký mã xác thực trong tệp thực thi đã ký mà không làm mất hiệu lực chữ ký. Gần đây, lỗ hổng này đã được sử dụng trong các cuộc tấn công chuỗi cung ứng vào phần mềm của hãng 3CX. Microsoft đã đưa ra bản vá về việc kiểm tra tính xác thực của chữ ký dưới dạng tùy chọn bật hoặc tắt, nếu không được cấu hình sẽ mặc định là tắt. Trong bản cập nhật này Microsoft đã bổ sung thêm các phiên bản hệ điều hành bị ảnh hưởng. Để nâng cao bảo mật an toàn thông tin cho các thiết bị sử dụng hệ điều hành Windows người dùng có thể xem xét việc bật tùy chọn kiểm tra này.

- 02 lỗ hổng bảo mật **CVE-2023-28287, CVE-2023-28295** trong Microsoft Publisher cho phép đối tượng tấn công thực thi mã từ xa.

- 02 lỗ hổng bảo mật **CVE-2023-28309, CVE-2023-28314** trong Microsoft Dynamics 365 cho phép đối tượng tấn công thực hiện tấn công XSS.

(Thông tin chi tiết các lỗ hổng bảo mật xin xem tại phụ lục kèm theo)

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan, đơn vị góp phần bảo đảm an toàn cho không gian mạng Việt Nam; thực hiện Công văn số 708/STTTT-BCVTCNTT ngày 20/4/2023 của Sở Thông tin và Truyền thông tỉnh Lai Châu về cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 4/2023, UBND huyện đề nghị các cơ quan, đơn vị thực hiện:

1. Kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công (tham khảo thông tin tại phụ lục kèm theo).

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

Trên đây là cảnh báo lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 4/2023, UBND huyện đề nghị các cơ quan, ban, ngành, đoàn thể huyện, UBND các xã, thị trấn quan tâm thực hiện. Trường hợp cần thiết, báo cáo về UBND huyện (qua Phòng Văn hóa và Thông tin - đồng chí Kiều Duy Thế Hoàn, số điện thoại 0984.258. 007) để có biện pháp khắc phục, xử lý kịp thời./. 

Nơi nhận:

- Như trên;
- Lãnh đạo UBND huyện;
- Lưu: VT. 

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Trần Quang Chiến

PHỤ LỤC

Thông tin về các lỗ hổng bảo mật trong sản phẩm Microsoft tháng 4/2023 (Kèm theo công văn số /UBND-PVH ngày tháng 4 năm 2023)

1. Thông tin các lỗ hổng bảo mật

TT	CVE	Mô tả	Link tham khảo
1	CVE-2023-28252	- Điểm: CVSS: 7.8 (cao) - Mô tả: lỗ hổng trong Windows Common Log File System Driver cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Windows Server, Windows 10,11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28252
2	CVE-2023-21554	- Điểm: CVSS: 9.8 (nghiêm trọng) - Mô tả: lỗ hổng trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21554
3	CVE-2023-23384 CVE-2023-23375 CVE-2023-28304	- Điểm: CVSS: 7.8/7.3 (cao) - Mô tả: lỗ hổng trong Microsoft SQL Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SQL Server, Microsoft ODBC Driver 18.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23384 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23375 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28304

4	CVE-2013-3900	- Điểm: CVSS: 7.4 (cao) - Mô tả: lỗ hổng xác thực chữ ký WinVerifyTrust cho phép đối tượng tấn công có thể thêm nội dung vào phần chữ ký mã xác thực trong tệp thực thi đã ký mà không làm mất hiệu lực chữ ký. - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900
5	CVE-2023-28287 CVE-2023-28295	- Điểm: CVSS: 8.8 (cao) - Mô tả: lỗ hổng trong Microsoft Publisher cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office, Microsoft Publisher.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28287 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28295
6	CVE-2023-28309 CVE-2023-28314	- Điểm: CVSS: 7.6/6.1 (cao) - Mô tả: lỗ hổng trong Microsoft Dynamics 365 cho phép đối tượng tấn công thực hiện tấn công XSS. - Ảnh hưởng: Microsoft Dynamics 365.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28309 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28314

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng bảo mật nói trên theo hướng dẫn của hãng. Quý đơn vị tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại link nguồn tham khảo tại mục 1 của phụ lục.

3. Tài liệu tham khảo

<https://msrc.microsoft.com/update-guide>

<https://www.zerodayinitiative.com/blog/2023/4/11/the-april-2023-security-update-review>