UBND HUYỆN VỊ XUYÊN
TIỂU BAN CHỈ ĐẠO AN TOÀN, AN NINH MẠNG

Số: 13 /TBCĐ-CA
V/v thông báo và hướng dẫn khắc phục lỗ hổng bảo mật trong các sản phẩm Microsoft công bố tháng 02/2024

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

Vị Xuyên, ngày 12 tháng 3 năm 2024

Kính gửi:

- Các cơ quan, ban, ngành huyện Vị Xuyên[1];
- Các tổ chức đoàn thể chính trị huyện;
- Các cơ sở giáo dục;
- UBND các xã, thị trấn;
- Các doanh nghiệp VT, CNTT trên địa bàn huyện;
- Các Nhà máy Thủy điện trên địa bàn huyện;
- Các hệ thống ngân hàng trên địa bàn huyện.

Theo thông báo của Bộ Công an, thời gian gần đây phát hiện một số lỗ hổng bảo mật có mức ảnh hưởng cao và nghiêm trọng. Theo đó, ngày 13/02/2024, Microsoft đã phát hành danh sách bản vá tháng 02 với 72 lỗ hổng an toàn thông tin trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt chú ý vào các lỗ hổng an toàn thông tin có mức ảnh hưởng cao và nghiêm trọng, cụ thể như sau:

- Lỗ hổng an toàn thông tin **CVE-2024-21410** trong Microsoft Exchange Sever cho phép đối tượng không cần xác thực thực hiện tấn công leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.

- 02 lỗ hổng an toàn thông tin **CVE-2024-21431**, **CV-2024-21378** trong Microsoft Outlook cho phép đối tượng không cần xác thực thực thi mã từ xa.

- Lỗ an toàn thông tin **CVE-2024-21399** trong Microsoft Edge (Chromium-based) cho phép đối tượng tấn công thực thi mã từ xa.

[1] Phòng Tài chính - Kế hoạch; Phòng Nông nghiệp và phát triển nông thôn; Phòng Nội vụ; Phòng Kinh tế - Hạ tầng; Phòng Văn hóa - Thông tin; Phòng Tài nguyên - Môi trường; Phòng Giáo dục - Đào tạo; Phòng Tư pháp; Phòng Lao động - TB&XH; Phòng Dân tộc; Ban Bồi thường GPMB; Ban Tổ chức; Ủy ban kiểm tra huyện ủy; Ban quản lý dự án ĐTXD; Ban Tuyên giáo; Ban Dân vận; Liên đoàn lao động huyện; Thanh tra huyện; Chi cục Thống kê; Chi cục Thuế; Tòa án Nhân dân huyện; Chi cục Thi hành án dân sự; Bảo hiểm xã hội; Kho bạc Nhà nước; Đội quản lý thị trường số 2; Hạt Kiểm lâm; Bệnh viện đa khoa huyện; BQL rừng đặc dụng Tây Côn Lĩnh; BQL rừng phòng hộ Phong Quang; Điện lực Vị Xuyên; Trung tâm dân số - KHHGĐ; Trung tâm Y tế; Trung tâm Văn hóa - TT&DL; Trung tâm dịch vụ CTN&MT; Trung tâm GDNN-GDTX; Trung tâm hành chính công; Trạm khuyến nông; Khu Kinh tế cửa khẩu Quốc tế Thanh Thủy; BQL Khu công nghiệp Bình Vàng.

- Lỗ hổng an toàn thông tin **CVE-2024-21412** trong Internet Shortcut Files cho phép đối tượng tấn công vượt qua cơ chế bảo mật. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2024-21379** trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-21384** trong Microsoft Ofifce OneNote cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-220673** trong Microsoft Ofifce OneNote cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-21351** trong Windows SmartScreen cho phép đối tượng tấn công vượt qua cơ chế bảo mật. Lỗ hổng hiện đang bị khai thác trong thực tế.

(Thông tin chi tiết các lỗ hổng bảo mật có tại phụ lục gửi kèm)

Để bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin trong hệ thống các cơ quan nhà nước trên địa bàn huyện; Tiểu Ban chỉ đạo An toàn, An ninh mạng huyện yêu cầu các cơ quan, đơn vị chỉ đạo bộ phận, cá nhân thực hiện những nội dung sau:

1. Tổ chức kiểm tra, rà soát và xác định máy tính trong phạm vi cơ quan, các đơn vị trực thuộc và UBND xã, thị trấn đang sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng *(nếu có)*, thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công *(link bản vá có tại phụ lục gửi kèm)*.

2. Tăng cường giám sát, sẵn sàng phương án xử lý, ứng cứu sự cố khi các thiết bị, máy chủ có dấu hiệu khai thác, tấn công mạng; đồng thời phổ biến, tuyên truyền kịp thời các nguy cơ về mất an toàn thông tin được cảnh báo của các cơ quan chức năng trong phạm vi cơ quan, địa phương.

Quá trình thực hiện, nếu gặp khó khăn, vướng mắc về kỹ thuật liên quan đến các nội dung, công việc trên đề nghị các đơn vị liên hệ với Công an huyện - Cơ quan Thường trực Tiểu Ban chỉ đạo *(Chi tiết liên hệ Đ/c Mai Thanh Tùng, cán bộ Đội An ninh, sđt 0972.091.886)* để phối hợp, hỗ trợ xử lý./.

Nơi nhận:
- Như trên;
- BCĐ An toàn, An ninh mạng Tỉnh (Phòng An ninh chính trị nội bộ - Công an tỉnh);
- VP HU; VP HĐND - UBND huyện;
- Vnptioffice;
- Lưu VT, AN, Tùng (TBCĐ).

TRƯỞNG TIỂU BAN CHỈ ĐẠO

CHỦ TỊCH UBND HUYỆN
Hoàng Thanh Tịnh

Phụ lục

THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG SẢN PHẨM CỦA MICROSOFT VÀ CÁC BẢN VÁ KHẮC PHỤC

(Kèm theo Công văn số /TBĐ-CA, ngày /3/2024)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Đường dẫn tham khảo
01	CVE-2024-21410	- Điểm: CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft Exchange Sever cho phép đối tượng không cần xác thực thực hiện tấn công leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft Exchange Sever 2016, 2019	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21410
02	CVE-2024-21431 CV-2024-21378	- Điểm: CVSS: 9.8 (nghiêm trọng) - Mô tả: Lỗ hổng Microsoft Outlook cho phép đối tượng không cần xác thực thực thi mã từ xa. - Ảnh hưởng: Microsoft Office, Microsoft Office LTSC, Microsoft 365 Apps for Enterprise, Microsoft Outlook.	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21413 http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21378
03	CVE-2024-21399	- Điểm: CVSS: 8.3 (Trung bình). - Mô tả: Lỗ hổng trong Microsoft Edge (Chromium-based) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21399

		Edge (Chromium-based)	
04	CVE-2024-21412	- Điểm: 8.1 (Cao) - Mô tả: Lỗ hổng trong Internet Shortcut Files cho phép đối tượng tấn công vượt qua cơ chế bảo mật. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Sever 2019, 2022.	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412
05	CVE-2024-21379	- Điểm: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Word, Microsoft Office, Microsoft Office LTSC, Microsoft 365 Apps for Enterprise.	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21379
06	CVE-2024-21384	- Điểm: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Ofifce OneNote cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft 365 Apps for Enterprise.	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21384
07	CVE-2024-220673	- Điểm: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office, Microsoft Office LTSC, Skype for Business.	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20673
		- Điểm: 7.6 (Cao) - Mô tả: Lỗ hổng trong Windows SmartScreen cho phép đối tượng tấn công vượt qua cơ chế bảo	http://msrc.microsoft.com/upda

08	CVE-2024-21351	mật. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Sever 2019, 2022.	te-guide/vulnerability/CVE-2024-21351

2. Hướng dẫn khắc phục

Biện pháp khắc phục là cập nhật bản vá cho các lỗ hổng bảo mật nói trên theo hướng dẫn của hãng Microsoft, các đơn vị tham khảo mẫu các bản cập nhật tương ứng cho các thiết bị, ứng dụng đang sử dụng tại đường dẫn nguồn tham khảo tại mục 1 của phụ lục./.