

SỞ THÔNG TIN VÀ TRUYỀN THÔNG CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
TỈNH THANH HÓA
TRUNG TÂM CNTT&TT
Độc lập - Tự do - Hạnh phúc

Số: /TTCNTT&TT-QTHT

Thanh Hoá, ngày tháng năm 2023

V/v lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 10/2023.

Kính gửi:

- Văn Phòng Tỉnh ủy;
- Văn Phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn Phòng UBND tỉnh;
- Các sở, ban, ngành cấp tỉnh;
- UBND các huyện, thị xã, thành phố;
- Các tổ chức đoàn thể chính trị cấp tỉnh;
- Các doanh nghiệp VT, CNTT trên địa bàn tỉnh.

Căn cứ Công văn số 1850/CATTT-NCSC ngày 19/10/2023 về việc lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 10/2023 của Cục An toàn thông tin Bộ Thông tin và Truyền thông. Theo đó ngày 10/10/2023, Microsoft đã phát hành danh sách bản vá tháng 10 với 103 lỗ hổng an toàn thông tin trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý vào các lỗ hổng an toàn thông tin có mức ảnh hưởng cao và nghiêm trọng sau:

- Lỗ hổng an toàn thông tin **CVE-2023-36778** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.

Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa, đã phát hành các văn bản cảnh báo về những lỗ hổng ảnh hưởng đến Microsoft Exchange Server. Điều này cho thấy Microsoft Exchange Server vẫn luôn là mục tiêu hàng đầu được các đối tượng tấn công có chủ đích nhắm đến. Vì vậy, để đảm bảo an toàn thông tin cho hệ thống của các cơ quan, tổ chức, Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa trân trọng đề nghị các đơn vị rà soát lỗ hổng liên quan đến Microsoft Exchange Server để phát hiện và có phương án xử lý kịp thời, đồng thời tăng cường giám sát nhằm giảm thiểu nguy cơ bị tấn công thông qua các lỗ hổng này.

- Lỗ hổng an toàn thông tin **CVE-2023-36563** trong Microsoft WordPad cho phép đối tượng tấn công thực hiện thu thập thông tin mã băm NTLM của người dùng. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2023-41763** trong Skype for Business cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai

thác trong thực tế.

- 02 lỗ hổng an toàn thông tin **CVE-2023-35349, CVE-2023-36697** trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2023-36434** trong Windows IIS Server cho phép đối tượng tấn công thực hiện leo thang đặc quyền.

Thông tin chi tiết các lỗ hổng bảo mật có tại phụ lục kèm theo.

(Thông tin chi tiết các lỗ hổng bảo mật có tại Phụ lục kèm theo.)

Để tăng cường chủ động phòng ngừa các rủi ro mất an toàn thông tin tại các hệ thống thông tin của các cơ quan, đơn vị, Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa đề nghị các cơ quan, đơn vị chỉ đạo các bộ phận, cá nhân thực hiện những nội dung sau:

1. Kiểm tra, rà soát, xác định máy sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng bởi các lỗ hổng bảo mật được công bố trên. Thực hiện cập nhật bản vá bảo mật đối với các lỗ hổng này kịp thời để tránh nguy cơ bị tấn công. Hướng dẫn kỹ thuật cách thức thực hiện chi tiết đối với lỗ hổng bảo mật tại địa chỉ: <https://attd.thanhhoa.gov.vn>

2. Chỉ đạo các Tổ ứng cứu sự cố an toàn thông tin mạng tại cơ quan, đơn vị mình tăng cường giám sát hoạt động các hệ thống thông tin và sẵn sàng phương án xử lý sự cố 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.

Trong quá trình thực hiện, nếu gặp khó khăn, vướng mắc về kỹ thuật liên quan đến các nội dung, công việc trên đề nghị liên hệ với Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa (*cơ quan thường trực của Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh*) để phối hợp hỗ trợ, xử lý.

Điện thoại: (0237)3718.699

Thư điện tử: ungcuusuco@thanhhoa.gov.vn

Xin trân trọng cảm ơn./.

Nơi nhận:

- Như kính gửi;
- Sở TT&TT (để b/c);
- PGĐ Sở Nguyễn Văn Tước (để b/c);
- Giám đốc Trung tâm (để b/c);
- Lưu: VT, QTHT.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Trần Ngọc Hưng

Phụ lục: Thông tin các lỗ hổng bảo mật
(Kèm theo công văn số /TTCNTT&TT-QTHT ngày tháng năm 2023
của Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-36778	<ul style="list-style-type: none"> - Điểm: CVSS: 8.0 (Cao) - Mô tả: Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Exchange Server 2016, 2019. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36778
2	CVE-2023-36563	<ul style="list-style-type: none"> - Điểm: CVSS: 6.5 (Cao) - Mô tả: Lỗ hổng trong Microsoft WordPad cho phép đối tượng tấn công thực hiện thu thập thông tin mã băm NTLM của người dùng. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36563
3	CVE-2023-41763	<ul style="list-style-type: none"> - Điểm: CVSS: 5.3 (Cao) - Mô tả: Lỗ hổng trong Skype for Business cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Skype for Business 2015, 2019. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-41763
4	CVE-2023-35349 CVE-2023-36697	<ul style="list-style-type: none"> - 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. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35349 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36697

STT	CVE	Mô tả	Link tham khảo
		- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	guide/vulnerability/CVE-2023-36697
5	CVE-2023-36434	- Điểm: CVSS: 9.8 (Cao) - Mô tả: Lỗ hổng trong Windows IIS Server cho phép đối tượng tấn công thực hiện leo thang đặc quyền. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36434

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng an toàn thông tin nói trên theo hướng dẫn của hãng. Hướng dẫn chi tiết khắc phục các lỗ hổng bảo mật trên tại địa chỉ: <https://attt.thanhhoa.gov.vn> (*Mục Hướng dẫn → Kỹ năng An toàn thông tin*). Các 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.

The image shows a screenshot of the website 'TRUNG TÂM ĐIỀU HÀNH AN TOÀN AN NINH MẠNG TỈNH THANH HÓA'. The navigation menu includes 'Trang chủ', 'Tin tức', 'Cảnh báo', 'Hướng dẫn', and 'Hỗ trợ'. The 'Hướng dẫn' menu item is highlighted with a red box, and a dropdown menu is visible below it, containing 'Kỹ năng an toàn thông tin', 'Công cụ', and 'Video'. The main content area features a blue background with a server rack and a laptop, and a headline: 'Dự báo sớm nguy cơ tấn công mạng trên diện rộng'. Below the headline, there is a paragraph of text and a red button that says 'BẤM VÀO ĐÂY ĐỂ XEM CHI TIẾT'.

3. Tài liệu tham khảo

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

<https://www.zerodayinitiative.com/blog/2023/10/10/the-october-2023-security-update-review>