

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 cảnh báo lỗ hổng bảo mật ảnh hưởng
Cao và Nghiêm trọng trong các sản phẩm
Microsoft công bố tháng 5/2023

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 729/CATTT-NCSC ngày 15/5/2023 về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 05/2023 của Cục An toàn thông tin, Bộ Thông tin và Truyền thông. Theo đó, ngày 09/05/2023, Microsoft đã phát hành danh sách bản vá tháng 05 với 38 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-2023-24955 trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

- 02 lỗ hổng bảo mật CVE-2023-29336, CVE-2023-24902 trong Win32k 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-2023-29325 trong Windows OLE cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đã được công bố rộng rãi trên Internet.

- Lỗ hổng bảo mật CVE-2023-24941 trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2023-24932 trong Secure Boot cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đã được công bố rộng rãi trên Internet.

- Lỗ hổng bảo mật CVE-2023-29344 trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2023-24953 trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

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

Đề 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://attt.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	Thông tin tham khảo
1	CVE-2023-24955	- Điểm: CVSS: 7.2 (cao) - Mô tả: lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24955
2	CVE-2023-29336 CVE-2023-24902	- Điểm: CVSS: 7.8 (cao) - Mô tả: lỗ hổng trong Win32k 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-2023-29336 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24902
3	CVE-2023-29325	- Điểm: CVSS: 8.1 (cao) - Mô tả: lỗ hổng trong Windows OLE cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đã được công bố rộng rãi trên Internet. - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29325
4	CVE-2023-24941	- Điểm: CVSS: 9.8 (ngghiêm trọng) - Mô tả: lỗ hổng trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24941

5	CVE-2023-24932	<ul style="list-style-type: none"> - Điểm: CVSS: 6.7 (trung bình) - Mô tả: lỗ hổng trong Secure Boot cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đã được công bố rộng rãi trên Internet. - Ảnh hưởng: Windows Server, Windows 10/11. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24932
6	CVE-2023-29344	<ul style="list-style-type: none"> - Điểm: CVSS: 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 365. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29344
7	CVE-2023-24953	<ul style="list-style-type: none"> - Điểm: CVSS: 7.8 (cao) - Mô tả: lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office, Microsoft 365, Microsoft Excel. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24953

2. Hướng dẫn khắc phục

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)



3. Tài liệu tham khảo

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

<https://www.zerodayinitiative.com/blog/2023/5/8/the-may-2023-security-update-review>