SỞ THÔNG TIN VÀ TRUYỀN THÔNG
THANH HÓA
TRUNG TÂM CNTT&TT

Số: 119 /TTCNTT&TT-QTHT
V/v lỗ hổng bảo mật ảnh hưởng Cao các sản phẩm Microsoft công bố tháng 8/2022

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

Thanh Hoá, ngày 19 tháng 8 năm 2022

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 viễn thông, CNTT trên địa bàn tỉnh.

Căn cứ Công văn số 1221/CATTT-NCSC ngày 10/8/2022 lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 8/2022 của Cục An toàn thông tin, Bộ Thông tin và Truyền thông. Ngày 09/8/2022, Microsoft đã phát hành danh sách bản vá tháng 8 với 121 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-2022-34713** trong Microsoft Windows Support Diagnostic Tool (MSDT) cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đang được khai thác rộng rãi trên Internet.

Tháng 6 vừa qua, lỗ hổng bảo mật CVE-2022-30190 có tên gọi là "Follina" liên quan đến Microsoft Windows Support Diagnostic Tool (MSDT) đã được các đối tượng tấn công khai thác rộng rãi. Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa cũng đã có cảnh báo cho lỗ hổng này tại văn bản số 80/TTCNTT&TT-QTHT về việc lỗ hổng bảo ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 6/2022. Cho thấy công cụ Microsoft Windows Support Diagnostic Tool (MSDT) vẫn đang là mục tiêu nhằm đến của nhiều đối tượng tấn công mạng. Các cơ quan, tổ chức cần đặc biệt quan tâm và có phương án khắc phục, xử lý kịp thời nếu bị ảnh hưởng.

- 04 lỗ hổng bảo mật **CVE-2022-21980, CVE-2022-24477, CVE-2022-24516**, **CVE-2022-30134** trong Microsoft Exchange Server cho phép đối tượng tấn công thu thập thông tin và thực hiện leo thang đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-35804** trong SMB Client and Server cho phép đối tượng tấn công thực thi mã từ xa trên phiên bản Windows 11.

- Lỗ hổng bảo mật **CVE-2022-34715** trong Windows Network File System cho phép

đối tượng tấn công chưa xác thực có thể thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-35742** trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ.

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 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. Thực hiện cập nhật bản vá 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. 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.

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

SỞ THÔNG TIN VÀ TRUYỀN THÔNG TỈNH THANH HÓA
TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Trần Ngọc Hưng

Phụ lục: Thông tin các lỗ hổng bảo mật

(Kèm theo công văn số /TTCNTT&TT-QTHT ngày tháng năm 2022 của Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa)

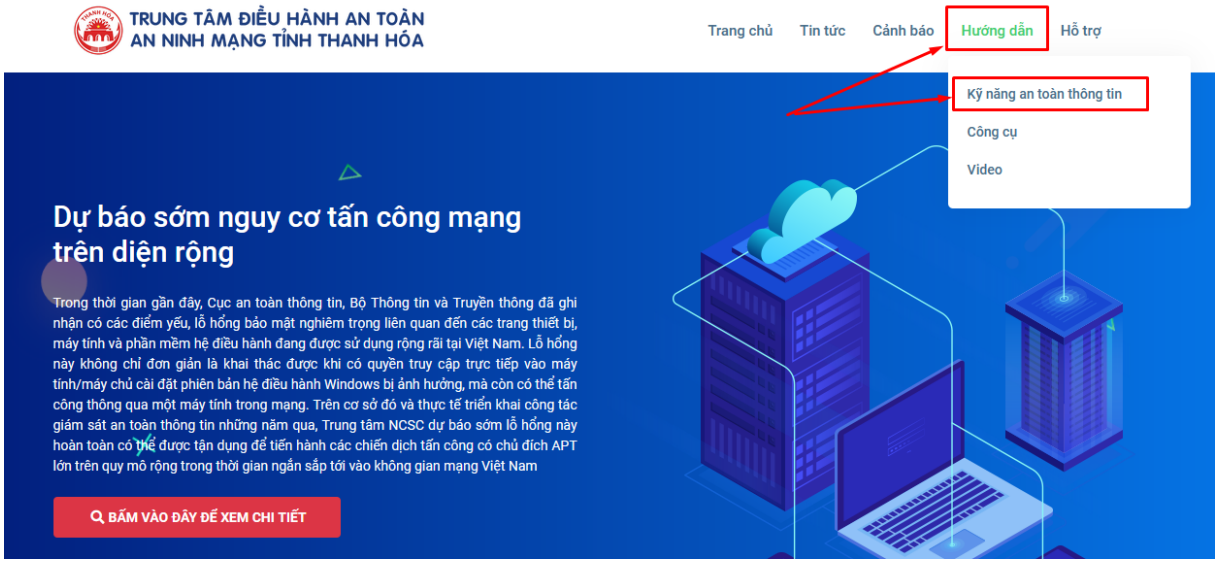
1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-34713	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft Windows Support Diagnostic Tool (MSDT) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34713
2	CVE-2022-21980 CVE-2022-24477 CVE-2022-24516 CVE-2022-30134	- Điểm CVSS: 8.0 (Cao) - Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thu thập thông tin và thực hiện leo thang đặc quyền. - Ảnh hưởng: Microsoft Exchange Server 2013/2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21980 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24477 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24516 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30134
3	CVE-2022-35804	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong SMB Client and Server cho phép đối tượng tấn công chưa xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows 11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35804
4	CVE-2022-34715	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows Network File System cho phép đối tượng tấn công chưa xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34715

5	CVE-2022-35742	- Điểm CVSS: 7.5 (Cao) - Lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ. - Ảnh hưởng: Microsoft Outlook 2012/2016, Microsoft Office LTSC 2021/2019, Microsoft 365 Apps.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35742

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/releaseNote/2022-Aug

https://www.zerodayinitiative.com/blog/2022/8/9/the-august-2022-security-update-review