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

Số: 80 /TTCNTT&TT-QTHT
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 6/2022

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

Thanh Hoá, ngày 20 tháng 6 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 VT, CNTT trên địa bàn tỉnh.

Căn cứ Công văn số 869/CATTT-NCSC ngày 16/6/2022 về việc cảnh báo lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 6/2022 của Cục An toàn thông tin, Bộ Thông tin và Truyền thông. Theo đó, ngày 14/6/2022, hãng Microsoft đã phát hành danh sách bản vá tháng 6 với 55 lỗ hổng bảo mật trong các sản phẩm của mình. Trong đó có 02 lỗ hổng bảo mật xếp loại mức độ ảnh hưởng ***Nghiêm trọng***, 07 lỗ hổng xếp loại ảnh hưởng mức độ ***Cao.*** Đây là những lỗ hổng có phạm vi ảnh hưởng tương đối lớn trên các sản phẩm của hãng Microsoft như hệ điều hành Windows phiên bản 7/8/10/11, phần mềm Microsoft Office. Đặc biệt là lỗ hổng bảo mật ***CVE-2022-30190*** (hay còn gọi là Follina) đã được Trung tâm Công nghệ thông tin và Truyền thông cảnh báo tại Công văn số 78/TTCNTT&TT-QTHT ngày 06/6/2021, lỗ hổng này hiện nay đã có mã khai thác tấn công cung cấp rộng rãi trên Internet, đang được các nhóm tấn công sử dụng để khai thác kiểm soát máy tính, thiết bị của người dùng, từ đó tấn công sâu hơn vào các hệ thống thông tin quan trọng khác.

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 bởi các lỗ hổng bảo mật được công bố trên. Đặc biệt là lỗ hổng bảo mật CVE-2022-30190 . 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. 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

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)

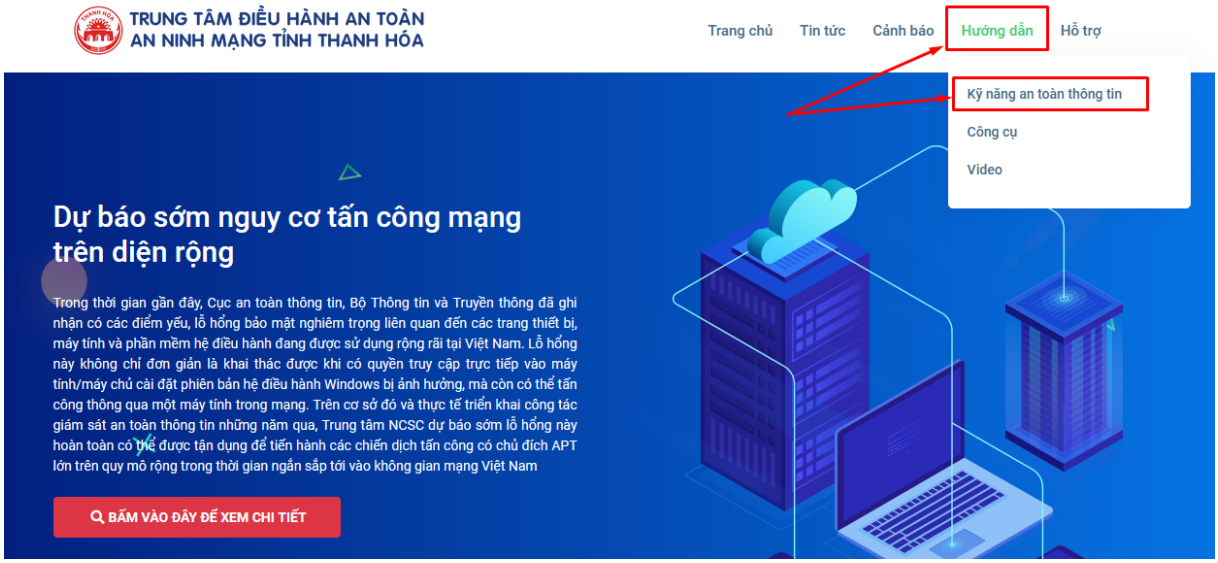
1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-30190 (Follina)	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Windows Microsoft Support Diagnotic Tool (MSDT) cho phép đối tượng tấn công thực thi mã tùy ý. - Ảnh hưởng: Windows 7/8.1/10, Windows Server 2008/2012/2016.	https: //msrc. micro soft. com/update-guide/en-US/vulnerability/CVE-2022-30190. Công văn số 78/TTCNTT&TT-QTHT về việc lỗ hổng bảo mật CVE-2022-30190 trong Microsoft Support Diagnostic Tool
2	CVE-2022-30136	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ trong Windows Network File System cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows Server 2012/2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30136
3	CVE-2022-30163	- Điểm CVSS: 8.5 (Cao) - Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2008/2012/2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30163
4	CVE-2022-30139	- Điểm CVSS:7.5 (cao) - Lỗ hổng trong Windows Lightweight Directory Access Protocol (LDAP) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows Server 2016/2019/2022.	https: //msrc. micro soft. com/update-guide/vulnerability/CV E-2022-30139

5	CVE-2022-30157 CVE-2022-30158	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: SharePoint Server 2019, SharePoint Enterprise Server 2016.	https: //msrc. micro soft. com/update-guide/vulnerability/CVE-2022-30157 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30158
6	CVE-2022-30165	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Windows Kerberos cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows 10/11, Windows Server 2016/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30165
7	CVE-2022-30173	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Excel 2013/2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30173
8	CVE-2022-30174	- Điểm CVSS: 7.4 (Cao) - Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft 365 Apps, Microsoft Office LTSC 2021.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30174

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-Jun

https://www.zerodayinitiative.com/blog/2022/6/14/the-june-2022-security-update-review