UBND TỈNH THỪA THIÊN HUẾ
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh Phúc

Số: 1855/STTTT-IOC
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 8/2022

Thừa Thiên Huế, ngày 12 tháng 8 năm 2022

Kính gửi:
- Văn phòng Tỉnh ủy;
- Các cơ quan chuyên môn thuộc UBND tỉnh;
- Các đơn vị sự nghiệp thuộc tỉnh;
- UBND các huyện, thị xã và thành phố Huế;
- Các cơ quan, đơn vị, tổ chức khác có kết kết mạng WAN.

Sở Thông tin và Truyền thông nhận được Công văn số 1221/CATTT-NCSC ngày 10/8/2022 của Cục An toàn thông tin về việc lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 8/2022.

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. Sở Thông tin và Truyền thông đã có cảnh báo cho lỗ hổng này tại văn bản số 1397/STTTT-IOC ngày 17/6/2022 về việc cảnh báo lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 6/2022. 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.

Nhằm đảm bảo an toàn thông tin, không để tin tặc tận dụng lỗ hổng bảo mật để tiến hành các cuộc vào hệ thống thông tin tập trung của tỉnh, Sở Thông tin và Truyền thông kính đề nghị quý đơn vị chủ động thực hiện các biện pháp sau:

1. Kiểm tra, rà soát, xác định máy tính/máy chủ 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 *(Thông tin chi tiết các lỗ hổng bảo mật có tại phụ lục kèm theo)*.

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 Sở Thông tin và Truyền thông và các cơ quan chức năng về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

Trong trường hợp cần hỗ trợ, quý đơn vị liên hệ đầu mối hỗ trợ của Sở Thông tin và Truyền thông:

- đ/c Hoàng Diên Kỷ; điện thoại: 0906 760 759;

email: hdky.stttt@thuathienhue.gov.vn

- đ/c La Thức; điện thoại: 0772 428 218;

email: lthuc.stttt@thuathienhue.gov.vn

Phòng Giám sát, điều hành an toàn, an ninh mạng - Trung tâm Giám sát, điều hành đô thị thông minh.

Trân trọng./.

Nơi nhận:
- Như trên;
- UBND tỉnh (để bc);
- Công an tỉnh (để p/h);
- BGĐ Sở;
- P.CNTT, HueIOC;
- Lưu: VT.

GIÁM ĐỐC

SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Xuân Sơn

Phụ lục
Thông tin về các lỗ hổng bảo mật Cao và Nghiêm trọng trong sản phẩm Microsoft công bố tháng 8/2022
(Kèm theo Công văn số 1855/STTTT-IOC ngày 12/8/2022 của Sở Thông tin và Truyền thông tỉnh Thừa Thiên Huế)

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.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35804

		- Ảnh hưởng: Windows 11.	
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

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng bảo mật nói trên theo hướng dẫn của hãng. Quý 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.

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