UBND TỈNH QUẢNG NGÃI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số 283 /STTTT-BCVT&CNTT

Quảng Ngãi, ngày 11 tháng 3 năm 2022

V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm Microsoft công bố tháng 3/2022

Kính gửi:
- Văn phòng: Tỉnh ủy, Đoàn ĐBQH&HĐND, UBND tỉnh;
- Các Sở, ban ngành; Hội, đoàn thể tỉnh;
- UBND các huyện, thị xã, thành phố;
- Báo Quảng Ngãi, Đài Phát thanh và Truyền hình tỉnh.

Theo cảnh báo của Cục An toàn thông tin tại Công văn số 315/CATTT-NCSC ngày 09/3/2022 về lỗ hổng bảo mật có mức ảnh hưởng Cao trong các sản phẩm Microsoft công bố tháng 03/2022; Sở Thông tin và Truyền thông đề nghị lãnh đạo các cơ quan, đơn vị chỉ đạo thực hiện một số biện pháp sau để hạn chế các rủi ro về nguy cơ mất an toàn thông tin:

1. Kiểm tra, rà soát máy chủ, máy trạm có sử dụng hệ điều hành Windows để phát hiện và xử lý kịp thời các máy chủ có khả năng bị ảnh hưởng bởi các lỗ hổng bảo mật sau:

- 02 lỗ hổng bảo mật **CVE-2022-21990, CVE-2022-23285** trong Remote Desktop Client cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đã có mã khai thác được công bố rộng rãi trên Internet.

- Lỗ hổng bảo mật **CVE-2022-24459** trong Windows Fax và Scan Service cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-24508** trong SMBv3 cho phép đối tượng tấn công thực thi mã từ xa trên Windows SMBv3 Client/Server.

- Lỗ hổng bảo mật **CVE-2022-23277** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa với tài khoản xác thực hợp lệ.

- Lỗ hổng bảo mật **CVE-2022-21967** trong Xbox Live Auth Manager for Windows cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-22006** trong HEVC Video Extensions cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-24501** trong cho phép đối tượng tấn công thực thi mã từ xa.

Đây là các lỗ hổng nguy hiểm, cần thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công ngay đối với các thiết bị bị ảnh hưởng theo hướng dẫn của Microsoft *(tham khảo thông tin lỗ hổng và cách khắc phục tại Phụ lục Thông tin về lỗ hổng bảo mật kèm theo Công văn này)*.

2. Khi phát hiện các hệ thống có biểu hiện bị khai thác, tấn công mạng, triển khai ngay các biện pháp xử lý ngăn chặn tấn công trên hệ thống và thông báo về Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi để có các biện pháp hỗ trợ, xử lý kịp thời.

Đề nghị lãnh đạo các cơ quan, đơn vị quan tâm chỉ đạo thực hiện./.

***Nơi nhận*:**
- Như trên;
- Phòng VH&TT các huyện, thị xã, thành phố;
- Thành viên Đội ứng cứu sự cố ATTT mạng tỉnh;
- Sở TT&TT: Lãnh đạo Sở, các phòng chuyên môn, TT CNTT&TT;
- Lưu: VT, BCVT&CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH QUẢNG NGÃI

Đỗ Quang Nghĩa

PHỤ LỤC

THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG MICROSOFT

(Kèm theo Công văn số /STTTT-BCVT&CNTT ngày /3/2022 của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-21990	- Điểm CVSS: 8.8(Cao) - Lỗ hổng trong Remote Desktop Client cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022, Windows 11/10/8.1/7.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-21990
2	CVE-2022-23285	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Remote Desktop Client cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022, Windows 10/8.1/7.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-23285
3	CVE-2022-24459	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng Windows Fax và Scan Service cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022, Windows 11/10/8.1/7.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-24459
4	CVE-2022-24508	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong trong SMBv3 cho phép đối tượng tấn công thực thi mã từ xa trên Windows SMBv3 Client/Server. - Ảnh hưởng: Windows 10/11, Windows Server 2022.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-24508

STT	CVE	Mô tả	Link tham khảo
5	CVE-2022-23277	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa với tài khoản xác thực hợp lệ. - Ảnh hưởng: Microsoft Exchange Server 2019/ 2016/2013.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-23277
6	CVE-2022-21967	- Điểm CVSS: 7.0 (Cao) - Lỗ hổng trong trong Xbox Live Auth Managerfor Windows cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows 10/11.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-21967
7	CVE-2022-22006	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong HEVC Video Extensions, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: HEVC Video Extensions.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-22006
8	CVE-2022-24501	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong VP9 Video Extensions, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: VP9 Video Extensions.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-24501

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/2022Mar
https://msrc.microsoft.com/update-guide/en-us