

UBND TỈNH TÂY NINH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: /STTTT-TTGSĐH
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng Cao
trong các sản phẩm Microsoft công bố
tháng 7/2022

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

Tây Ninh, ngày tháng 7 năm 2022

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các cơ quan tham mưu, giúp việc Tỉnh ủy;
- Mặt trận Tổ quốc và các Đoàn thể chính trị - xã hội;
- Các Sở, ban, ngành tỉnh;
- Các huyện, thị, thành ủy;
- UBND các huyện, thị xã, thành phố.

Thực hiện theo Công văn số 1071/CATTT-NCSC của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc cảnh báo lỗ hổng bảo mật Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 7/2022 (*Chi tiết lỗ hổng trong phụ lục kèm theo*).

Nhằm đảm bảo an toàn thông tin cho người dùng, đơn vị và toàn bộ hệ thống của tỉnh, Sở Thông tin và Truyền thông đề nghị các đơn vị, địa phương thực hiện gấp các công việc cụ thể như sau:

1. Kiểm tra, xác định các thiết bị máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời theo hướng dẫn tại phụ lục để tránh nguy cơ bị tấn công.
2. Tăng cường kiểm tra, giám sát và sẵn sàng phương án 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.

Thông tin liên quan đề nghị liên hệ Ông Vương Duy Thanh - Trung tâm Giám sát, điều hành kinh tế, xã hội tập trung; Điện thoại: 0932624462.

Trân trọng./.

Nơi nhận:

- Như trên;
- GD Sở (b/c);
- P. CNTTBCVT;
- Lưu: VT, TTGSĐH.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

PHỤ LỤC

CÁC LỖ HỒNG BẢO MẬT CAO VÀ NGHIÊM TRỌNG TRONG CÁC SẢN PHẨM MICROSOFT CÔNG BỐ THÁNG 7/2022

1. Thông tin về các lỗ hổng

Ngày 12/7/2022, Microsoft đã phát hành danh sách bản vá tháng 7 với 84 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 sau:

- Lỗ hổng bảo mật **CVE-2022-22047** trong Windows Client Server Run-Time Subsystem cho phép đối tượng tấn công thực hiện leo thang đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-30216** trong Windows Server Service cho phép đối tượng tấn công cài chứng chỉ giả mạo độc hại lên máy chủ mục tiêu từ đó có thể thực hiện các dạng tấn công khác bao gồm tấn công chiếm quyền điều khiển.

- Lỗ hổng bảo mật **CVE-2022-22038** trong Remote Procedure Call Runtime cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa.

- 02 Lỗ hổng bảo mật **CVE-2022-22029, CVE-2022-22039** trong Windows Network File System cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa.

- 04 lỗ hổng bảo mật **CVE-2022-22022, CVE-2022-22041, CVE-2022-30206, CVE-2022-30226** trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. Khai thác thành công, CVE-2022-22041 và CVE-2022-30226 cho phép đối tượng tấn công chiếm quyền điều khiển hệ thống; CVE-2022-22022 và CVE-2022-30226 chỉ cho phép đối tượng tấn công xóa tệp tùy ý trên hệ thống mục tiêu.

Thông tin chi tiết các lỗ hổng bảo mật:

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-22047	<ul style="list-style-type: none">- Điểm CVSS: 7.8 (Cao)- Lỗ hổng trong Windows Client Server Run-Time Subsystem cho phép đối tượng tấn công thực hiện leo thang đặc quyền.- Ảnh hưởng: Windows 7/8.1/10/11. Windows Server 2008/2012.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22047
2	CVE-2022-30216	<ul style="list-style-type: none">- Điểm CVSS: 8.8 (Cao)- Lỗ hổng trong Windows Server Service cho phép đối tượng tấn công cài chứng chỉ giả mạo độc hại lên máy chủ mục tiêu từ đó có	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30216

		<p>thể thực hiện các dạng tấn công khác bao gồm tấn công chiếm quyền điều khiển.</p> <ul style="list-style-type: none"> - Ảnh hưởng: Windows 10/11, Windows Server. 	y/CVE-2022-30216
3	CVE-2022-22029	<ul style="list-style-type: none"> - Điểm CVSS: 8.1 (Cao) - Lỗ hổng 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 2008/2012/2016/2019/2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22029
4	CVE-2022-22039	<ul style="list-style-type: none"> - Điểm CVSS: 7.5 (Cao) - Lỗ hổng 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 2008/2012/2016/2019/2022. 	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-22039
5	CVE-2022-22038	<ul style="list-style-type: none"> - Điểm CVSS: 8.1 (Cao) - Lỗ hổng trong Remote Procedure Call Runtime cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22038
6	CVE-2022-30206	<ul style="list-style-type: none"> - Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows 7/8.1/10, Windows Server 2008/2012/2019/2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30206
7	CVE-2022-22022	<ul style="list-style-type: none"> - Điểm CVSS: 7.1 (Cao) - Lỗ hổng trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2016/2019/2022. 	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-22022

8	CVE-2022-30226	<ul style="list-style-type: none"> - Điểm CVSS: 7.1 (Cao) - Lỗ hổng trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/12, Windows Server 2008/2012/2019/2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30226
9	CVE-2022-22041	<ul style="list-style-type: none"> - Điểm CVSS: 6.8 (Cao) - Lỗ hổng trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows 8.1/10, Windows Server 2012/2016/2019/2022. 	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-22041

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-Jul>
<https://www.zerodayinitiative.com/blog/2022/7/12/the-july-2022-security-update-review>