

Số: /TTCNTT-KTHT
V/v lỗ hổng bảo mật ảnh hưởng Cao và
Nghiêm trọng trong các sản phẩm
Microsoft công bố tháng 8/2022

Hà Nội, ngày tháng năm 2022

Kính gửi: Các đơn vị trực thuộc Bộ

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 cũng đã có cảnh báo cho lỗ hổng này tại Công văn số 217/TTCNTT-KTHT về việc lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 6/2022 phát hành ngày 21/6/2022. 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.

Nhằm bảo đảm an toàn thông tin cho hệ thống thông tin của Quý đơn vị, Trung tâm Công nghệ thông tin khuyến nghị Quý đơn vị thực hiện:

1. Kiểm tra, rà soát, xác định máy tính 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 (tham khảo thông tin 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 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 trường hợp cần thiết, Quý đơn vị liên hệ đầu mối hỗ trợ của Trung tâm Công nghệ thông tin: Phòng Kỹ thuật hạ tầng, điện thoại 024.39439060, thư điện tử: phongktht@most.gov.vn.

Trân trọng./.

Nơi nhận:

- Như trên;
- Thứ trưởng Bùi Thế Duy (để b/c);
- Cổng thông tin điện tử Bộ KH&CN;
- Lưu: VT, KTHT.

GIÁM ĐỐC

Hà Quốc Trung

Phụ lục
Thông tin về các lỗ hổng bảo mật trong sản phẩm Microsoft
(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2022 của Trung tâm
Công nghệ thông tin)

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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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. Nguồn 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>

DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN

(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2022 của Trung tâm Công nghệ thông tin)

TT	Tên đơn vị
1.	Vụ Khoa học Xã hội, Nhân văn và Tự nhiên
2.	Vụ Khoa học và Công nghệ các ngành kinh tế - kỹ thuật
3.	Vụ Đánh giá, Thẩm định và Giám định công nghệ
4.	Vụ Công nghệ cao
5.	Vụ Kế hoạch - Tài chính
6.	Vụ Pháp chế
7.	Vụ Tổ chức cán bộ
8.	Vụ Hợp tác quốc tế
9.	Vụ Thi đua - Khen thưởng
10.	Vụ Phát triển khoa học và công nghệ địa phương
11.	Văn phòng Bộ
12.	Thanh tra Bộ
13.	Cục Công tác phía Nam
14.	Cục Ứng dụng và phát triển công nghệ
15.	Cục Năng lượng nguyên tử
16.	Cục Thông tin Khoa học và Công nghệ Quốc gia
17.	Cục Phát triển thị trường và doanh nghiệp khoa học và công nghệ
18.	Cục An toàn bức xạ và hạt nhân
19.	Cục Sở hữu trí tuệ
20.	Tổng cục Tiêu chuẩn Đo lường Chất lượng
21.	Ban quản lý khu công nghệ cao Hoà Lạc
22.	Học viện Khoa học, Công nghệ và Đổi mới sáng tạo
23.	Viện Khoa học và công nghệ Việt Nam - Hàn Quốc (VKIST)
24.	Viện Nghiên cứu sáng chế và Khai thác công nghệ
25.	Viện Năng lượng nguyên tử Việt Nam
26.	Viện Ứng dụng công nghệ
27.	Viện Đánh giá khoa học và Định giá công nghệ
28.	Viện Khoa học sở hữu trí tuệ
29.	Viện Nghiên cứu và Phát triển Vùng
30.	Văn phòng các Chương trình trọng điểm cấp nhà nước

31.	Văn phòng Công nhận chất lượng
32.	Văn phòng Đăng ký hoạt động khoa học và công nghệ
33.	Văn phòng các Chương trình khoa học và công nghệ quốc gia
34.	Báo điện tử Tin nhanh Việt Nam (VnExpress)
35.	Tạp chí Khoa học và Công nghệ Việt Nam
36.	Nhà xuất bản Khoa học và Kỹ thuật
37.	Quỹ Phát triển khoa học và công nghệ quốc gia
38.	Quỹ Đổi mới công nghệ quốc gia
39.	Trung tâm Nghiên cứu và Phát triển truyền thông khoa học và công nghệ
40.	Trung tâm Nghiên cứu và Phát triển hội nhập khoa học và công nghệ quốc tế