

Số: /TTCNTT-KTHT
V/v lỗ hổng bảo mật ảnh hưởng cao và
nghiêm trọng trong các sản phẩm Microsoft
công bố tháng 11/2021

Hà Nội, ngày tháng 11 năm 2021

Kính gửi: Các đơn vị trực thuộc Bộ

Ngày 10/11/2021, Microsoft đã phát hành danh sách bản vá tháng 11 với 55 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 sau:

- Lỗ hổng bảo mật **CVE-2021-42321** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa. Không giống như các lỗ hổng zero-day liên quan đến các vụ tấn công hàng loạt hệ thống Exchange Server vào đầu năm nay, để khai thác lỗ hổng CVE-2021-42321 kẻ tấn công cần xác thực vào hệ thống mục tiêu. Tuy vậy theo Cục An toàn thông tin – Bộ Thông tin và Truyền thông, Microsoft Exchange Server luôn là một mục tiêu ưa thích của các nhóm tấn công mạng vì vậy các đơn vị cần có kế hoạch cập nhập sớm các hệ thống bị ảnh hưởng.

- 02 lỗ hổng bảo mật **CVE-2021-38631, CVE-2021-41371** trong Microsoft Remote Desktop Protocol (RDP): ảnh hưởng đến Windows 7 đến Windows 11 và trên Windows Server 2008-2019, cho phép đối tượng tấn công có thể thu thập thông tin mật khẩu RDP của hệ thống dễ bị tấn công.

- Lỗ hổng bảo mật **CVE-2021-42292** trong Microsoft Excel ảnh hưởng đến Microsoft Excel phiên bản 2013-2021, cho phép đối tượng tấn công cài cắm mã độc chỉ bằng cách lợi dụng người dùng mở một tệp Excel độc hại.

- Lỗ hổng bảo mật **CVE-2021-26443** trong Microsoft Virtual Machine Bus (VMBus) cho phép đối tượng tấn công thực thi mã từ xa.

- 02 lỗ hổng bảo mật **CVE-2021-43208, CVE-2021-43209** trong 3D Viewer: cho phép đối tượng tấn công thực thi mã từ xa.

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 nhập 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);
- Công 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 / /2021 của Trung tâm
Công nghệ thông tin)

1. Thông tin các lỗ hổng bảo mật

TT	CVE	Mô tả	Link tham khảo
1	CVE-2021-42321	- CVSS: 8.8 (cao) - Lỗ hổng trong Microsoft Exchange Server. Khai thác lỗ hổng này đối tượng tấn công cần xác thực để thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-42321
2	CVE-2021-42292	- CVSS: 7.8 (cao) - Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công cài cắm mã độc chỉ bằng cách lợi dụng người dùng mở một tệp Excel độc hại.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-42292
3	CVE-2021-43209 CVE-2021-43208	- CVSS: 7.8 (cao) - Lỗ hổng trong 3D Viewer cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43209 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43208
4	CVE-2021-38631 CVE-2021-41371	- CVSS: 4.4 (Trung bình) - Lỗ hổng trong Windows Remote Desktop Protocol (RDP) cho phép đối tượng tấn công thu thập thông tin.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38631 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-41371
5	CVE-2021-26443	- CVSS: 9.0 (cao) - Lỗ hổng trong Microsoft Virtual Machine Bus (VMBus) cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26443

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/2021-Nov>

DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN

(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2021 của Trung tâm Công nghệ thông tin)

TT	Tên đơn vị
1.	Thanh tra Bộ
2.	Cục Công tác phía Nam
3.	Cục Ứng dụng và phát triển công nghệ
4.	Cục Năng lượng nguyên tử
5.	Cục Thông tin Khoa học và Công nghệ Quốc gia
6.	Cục Phát triển thị trường và doanh nghiệp khoa học và công nghệ
7.	Cục An toàn bức xạ và hạt nhân
8.	Cục Sở hữu trí tuệ
9.	Tổng Cục tiêu chuẩn đo lường chất lượng
10.	Ban quản lý khu công nghệ cao Hoà Lạc
11.	Học viện Khoa học, Công nghệ và Đổi mới sáng tạo
12.	Viện Khoa học và công nghệ Việt Nam - Hàn Quốc (VKIST)
13.	Viện Nghiên cứu sáng chế và Khai thác công nghệ
14.	Viện Năng lượng nguyên tử Việt Nam
15.	Viện Ứng dụng công nghệ
16.	Viện Đánh giá khoa học và Định giá công nghệ
17.	Viện Khoa học sở hữu trí tuệ
18.	Viện Nghiên cứu và Phát triển Vùng
19.	Văn phòng các Chương trình trọng điểm cấp nhà nước
20.	Văn phòng Công nhận chất lượng
21.	Văn phòng Đăng ký hoạt động khoa học và công nghệ
22.	Văn phòng các Chương trình khoa học và công nghệ quốc gia
23.	Báo Khoa học và Phát triển
24.	Tạp chí Khoa học và Công nghệ Việt Nam
25.	Nhà xuất bản Khoa học và Kỹ thuật
26.	Quỹ Phát triển khoa học và công nghệ quốc gia
27.	Quỹ Đổi mới công nghệ quốc gia
28.	Trung tâm Nghiên cứu và Phát triển truyền thông khoa học và công nghệ
29.	Trung tâm Nghiên cứu và Phát triển hội nhập khoa học và công nghệ quốc tế