BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Số: 616 /TTCNTT-HTATTT
V/v lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 11/2024

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

Hà Nội, ngày 26 tháng 11 năm 2024

Kính gửi: Các đơn vị trực thuộc Bộ
(Danh sách kèm theo)

Ngày 12/11/2024, Microsoft đã phát hành danh sách bản vá tháng 11/2024 với **92 lỗ hổng an toàn thông tin** gồm có **89 lỗ hổng an toàn thông tin** trong các sản phẩm của hãng Microsoft và **03 lỗ hổng an toàn thông tin** trong các sản phẩm thuộc bên thứ ba có ảnh hưởng tới Microsoft, Trong đó có 04 lỗ hổng mức Nghiêm trọng và 84 lỗ hổng mức độ Cao:

Các lỗ hổng này có mức độ ảnh hưởng **Cao** và **Nghiêm trọng**, có thể bị đối tượng tấn công khai thác để thực hiện các hành vi trái phép, gây ra nguy cơ mất an toàn thông tin và ảnh hưởng đến các hệ thống thông tin của đơn vị.

Lỗ hổng an toàn thông tin tồn tại trên một số sản phẩm của Microsoft như: Windows và các thành phần của Windows; Office và các thành phần của Office; Azure; .NET và Visual Studio; LightGBM; Exchange Server; SQL Server; TorchGeo; Hyper-V; Windows VMSwitch.

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

1. Kiểm tra, rà soát, xác định máy sử dụng sản phẩm của Microsoft 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 có thể liên hệ đầu mối hỗ trợ của Trung tâm Công nghệ thông tin: Phòng Hạ tầng và an toàn thông tin, 113 Trần Duy Hưng, Trung Hòa, Cầu Giấy, Hà Nội; số điện thoại: 024.39439060; địa chỉ thư điện tử: phongktht@most.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Bùi Thế Duy (để b/c);
- Giám đốc (để b/c);
- Cổng thông tin điện tử của Bộ (để đăng tải);
- Lưu: VT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Ngô Minh Phước

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG SẢN PHẨM MICROSOFT
(Kèm theo Công văn số 616 /TTCNTT-HTATTT ngày 26 / 11 /2024 của Trung tâm Công nghệ thông tin)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-43639	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Kerberos cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: **Máy tính** cài đặt Windows 10, Windows 11, **Hệ thống** cài đặt Windows Server 2012, 2016, 2019, 2022, 2025.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43639
2	CVE-2024-43498	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong .NET và Visual Studio cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: **Máy tính** hoặc **Hệ thống** cài đặt .NET 9.0, Microsoft Visual Studio 2022.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43498
3	CVE-2024-49039	- Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Windows Task Scheduler cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: **Máy tính** cài đặt Windows 10, Windows 11, **Hệ thống** cài đặt Windows Server 2016, 2019, 2022, 2025.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-49039

4	CVE-2024-43625	- Điểm CVSS: 8.1 (Cao) - Mô tả: Lỗ hổng trong Microsoft Windows VMSwitch cho phép đối tượng tấn công thực hiện leo thang đặc quyền. - Ảnh hưởng: **Máy tính** cài đặt Windows 10, Windows 11, **Hệ thống** cài đặt Windows Server 2022, 2025.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43625
5	CVE-2024-49026 CVE-2024-49027 CVE-2024-49028 CVE-2024-49029 CVE-2024-49030	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: **Máy tính** hoặc **Hệ thống** cài đặt Microsoft Office Online Server, Microsoft Excel 2016 Click-to-Run, Microsoft Office LTSC 2021, 2024, Microsoft 365 Apps for Enterprise, Microsoft Office 2019.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-49026 https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-49027 https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-49028 https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-49029 https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-49030
6	CVE-2024-49019	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Active Directory Certificate Services phép đối tượng tấn công thực hiện leo thang đặc quyền. Thông tin chi tiết về lỗ hổng đã được công bố công khai. - Ảnh hưởng: **Hệ thống** cài đặt Windows Server 2008, 2012, 2016, 2019, 2022, 2025	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-49019

7	CVE-2024-49040	- Điểm CVSS: 7.5 (Cao) - Mô tả: Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). Thông tin chi tiết về lỗ hổng đã được công bố công khai. - Ảnh hưởng: **Hệ thống** cài đặt Microsoft Exchange Server 2016, 2019.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-49040
8	CVE-2024-43451	- Điểm CVSS: 6.5 (Trung bình) - Mô tả: Lỗ hổng trong Windows gây lộ lọt mã băm NTLM, cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: **Máy tính** cài đặt Windows 10, Windows 11, **Hệ thống** cài đặt Windows Server 2016, 2019, 2022, 2025.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43451

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng an toàn thông tin 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/

https://www.zerodayinitiative.com/blog/2024/11/12/the-november-2024-security-update-review

DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN

(Kèm theo Công văn số 616/TTCNTT-HTATTT ngày 26/11/2024 của Trung tâm Công nghệ thông tin)

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