SỞ THÔNG TIN VÀ TRUYỀN THÔNG
CAO BẰNG
TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 132 /TTCNTTTT-KTCCN

V/v cảnh báo 10 lỗ hổng bảo mật mức cao và nghiêm trọng trong các sản phẩm Microsoft

Cao Bằng, ngày 16 tháng 8 năm 2021

Kính gửi:

- Văn phòng Tỉnh uỷ;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các sở, ban, ngành, UBND các huyện và thành phố;
- Toà án nhân dân tỉnh, Viện kiểm sát nhân dân tỉnh;
- Cục thuế tỉnh, Cục Hải quan tỉnh, Cục Quản lý thị trường tỉnh, Bảo hiểm xã hội tỉnh.

Thực hiện chức năng, nhiệm vụ được giao, qua hoạt động điều phối, hợp tác và chia sẻ thông tin của Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia, Trung tâm Công nghệ thông tin và Truyền thông Cao Bằng nhận được cảnh báo tại Công văn số 1115/CATTT-NCSC ngày 13/8/2021 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc 10 lỗ hổng bảo mật mức cao và nghiêm trọng trong các sản phẩm Microsoft.

Ngày 10/8/2021, Microsoft phát hành danh sách bản vá lỗi tháng 8/2021 với 44 bản vá cho các lỗ hổng bảo mật trong sản phẩm của mình, 13 trong số 44 lỗ hổng được công bố lần này là lỗ hổng bảo mật cho phép thực thi mã từ xa, 7 lỗ hổng trong số này được đánh giá là quan trọng. Trong đó đáng chú ý là **10** lỗ hổng bảo mật có mức ảnh hưởng tương đối lớn trong các sản phẩm Microsoft (*Thông tin chi tiết lỗ hổng và hướng dẫn khắc phục có tại phụ lục kèm theo),* đặc biệt là **04** lỗ hổng bảo mật tồn tại trong Windows Print Spooler và Microsoft Windows. Cụ thể như sau:

- 03 lỗ hổng bảo mật (**CVE-2021-36936, CVE-2021-36947, CVE-2021-34483)** trong Windows Print Spooler: cho phép đối tượng tấn công thực thi mã từ xa, nâng cao đặc quyền. Trong 2 tháng vừa qua, lỗ hổng trong Print Spooler đã có ảnh hưởng khá lớn và được quan tâm đặc biệt khi mà Microsoft liên tục công bố bản vá cho các lỗ hổng liên quan, bắt đầu với CVE-2021-1675 vào tháng 6, tiếp theo là bản vá lỗi cho CVE-2021-34527 (còn được gọi là PrintNightmare) vào tháng 7. Công cụ để khai thác các lỗ hổng trên đã được công bố rộng rãi trên Internet nên nguy cơ bị khác thác bởi các nhóm tấn công APT hoặc được sử dụng trong các cuộc tấn công diện rộng là rất lớn. 02 lỗ hổng này đã được cảnh báo tại

văn bản số 2604/BTTT-CATTT ngày 16/7/2021 về việc 05 lỗ hổng bảo mật mức cao và nghiêm trọng trong các sản phẩm Microsoft phát hành và văn bản số 2210/BTTTT-CATTT ngày 22/6/2021 về việc dự báo sớm nguy cơ tấn công mạng trên diện rộng.

- Lỗ hổng bảo mật **(CVE-2021-26424)** trong Microsoft Windows: là lỗ hổng TCP/IP, cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này ảnh hưởng đến Windows 7 đến 10 và Windows Server 2008 đến 2019 với điểm CVSS: 9.9 (Nghiêm trọng). Tuy vậy theo dự đoán của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), mã khai thác của lỗ hổng này sẽ khó được công bố sớm do việc phát triển mã khai thác phải vượt qua các tính năng bảo vệ trong các phiên bản mới của Windows.

Nhằm đảm bảo an toàn thông tin cho hệ thống của quý đơn vị, Trung tâm Công nghệ thông tin và Truyền thông kính đề nghị quý cơ quan, đơn vị thực hiện một số nội dung sau:

1. Kiểm tra, rà soát và xác định máy chủ, máy trạm sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá bảo mật cho các máy bị ảnh hưởng theo hướng dẫn của Microsoft *(chi tiết tham khảo 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 ứng cứu sự cố máy tính tỉnh Cao Bằng: Trung tâm Công nghệ thông tin và Truyền thông Cao Bằng, Địa chỉ: Số 009, Hoàng Văn Thụ, Hợp Giang, thành phố Cao Bằng, Điện thoại: 02063.955.899. Email: cbitc@caobang.gov.vn.

Đề nghị quý cơ quan, đơn vị quan tâm triển khai thực hiện./.

GIÁM ĐỐC

SỞ THÔNG TIN VÀ TRUYỀN THÔNG TỈNH CAO BẰNG
TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Triệu Đình Thăng

Nơi nhận:
- Như trên;
- Lãnh đạo Sở TTTT (b/c);
- Phòng BCVT-CNTT;
- Lưu: VT, KTCN.

Phụ lục

Thông tin lỗ hổng bảo mật

(Kèm theo Công văn số: *132* /TTCNTTTT-KTCCN *ngày 16/8/2021*

của Trung tâm Công nghệ thông tin và Truyền thông Cao Bằng)

1. Thông tin lỗ hổng bảo mật

TT	CVE	Mô tả	Ghi chú
1	CVE-2021-36947	- Lỗ hổng tồn tại trong Windows Print Spooler, cho phép đối tượng tấn công thực thi mã từ xa. - Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Windows 7/8.1/10 và Windows Server 2008/2012/2019.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36947
	CVE-2021-36936	- Lỗ hổng tồn tại trong Windows Print Spooler, cho phép đối tượng tấn công thực thi mã từ xa. - Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Windows 7/8.1/10 và Windows Server 2008/2012/2019.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36936
	CVE-2021-34483	- Lỗ hổng tồn tại trong Windows Print Spooler, cho phép đối tượng tấn công nâng cao đặc quyền. - Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Windows 7/8.1/10 và Windows Server 2008/2012/2016.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34483
2	CVE-2021-26424	- Lỗ hổng tồn tại liên quan đến giao thức TCP/IP của Windows, cho phép đối tượng tấn công thực thi mã từ xa. - Điểm CVSS: 9.9 (Nghiêm trọng)	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26424

		- Ảnh hưởng: Windows 7 đến 10 và Windows Server 2008 đến 2019.	
3	CVE-2021-34535	- Lỗ hổng tồn tại trong Remote Desktop Client, cho phép đối tượng tấn công thực thi mã từ xa. - Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Windows 7/8.1/10 và Windows Server 2008/2012/2019.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34535
4	CVE-2021-36948	- Lỗ hổng tồn tại trong Windows Update Medic Service (WaasMedic), cho phép đối tượng tấn công nâng cao đặc quyền. - Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Windows 10 và Windows Server 2019.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36948
5	CVE-2021-36942	- Lỗ hổng tồn tại trong Windows Local Security Authority (LSA), cho phép đối tượng tấn công thực hiện tấn công giả mạo. - Điểm CVSS: 7.5 (Cao) - Ảnh hưởng: Windows 10 và Windows Server 2019.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36942
6	CVE-2021-36941	- Lỗ hổng tồn tại trong Microsoft Word, cho phép đối tượng tấn công thực thi mã từ xa. - Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Microsoft 365, Microsoft Office 2019.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36941
7	CVE-2021-34478	- Lỗ hổng tồn tại trong Microsoft Office, cho phép đối tượng tấn công thực thi mã từ xa. - Điểm CVSS: 7.8 (Cao)	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34478

		- Ảnh hưởng: Microsoft 365, Microsoft Office 2019.	
8	CVE-2021-34524	- Lỗ hổng tồn tại trong Microsoft Dynamics 365 (on-premises), cho phép đối tượng tấn công thực thi mã từ xa. - Điểm CVSS: 8.1 (Cao) - Ảnh hưởng: Microsoft Dynamics 365 (on-premises) version 9.0 và 9.1	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34524
9	CVE-2021-26426	- Lỗ hổng tồn tại trong Windows User Profile Service cho phép đối tượng tấn công nâng cao đặc quyền. - Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Windows Server 2008/2012/2016/2019, Windows 7/8.1/10	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26426
10	CVE-2021-34484	- Lỗ hổng tồn tại trong Windows User Profile Service cho phép đối tượng tấn công nâng cao đặc quyền. - Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Windows Server 2008/2012/2016/2019, Windows 7/8.1/10	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34484

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục lỗ hổng bảo mật này là cập nhật bản vá. Trong trường hợp chưa thể cập nhật bản vá kịp thời, Quý đơn vị thực hiện các biện pháp khắc phục theo hướng dẫn của hãng, để giảm thiểu nguy cơ tấn công (tham khảo tại nguồn link được thống kê ở bảng trên)

3. Nguồn tham khảo

- Bản vá tháng 8 của Microsoft:

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

https://msrc.microsoft.com/update-guide/releaseNote/2021-Aug