Phụ lục

Thông tin lỗ hổng bảo mật

(Kèm theo Công văn số 2609/BTTTT-CATTT ngày 16 / 7 /2021 của Bộ Thông tin và Truyền thông)

1. Thông tin lỗ hổng bảo mật

TT	CVE	Mô tả	Ghi chú
1	CVE-2021-34473	- **Mô tả:** Lỗ hổng tồn tại trong Microsoft Exchange Server, cho phép đối tượng tấn công thực thi mã từ xa. - **Điểm CVSS:** 9.1 (cao) - **Ảnh hưởng:** Exchange Server 2019/2016/2013 - **Nguồn tham khảo:** https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473	- Công văn số 13/NCSC-ĐTPT về việc lỗ hổng bảo mật trong Microsoft Exchange Server ngày 03/3/2021. - Công văn số 1122/BTTTT-CATTT về việc 04 lỗ hổng bảo mật mới ảnh hưởng nghiêm trọng tới máy chủ thư điện tử Microsoft Exchange Server và hướng dẫn xử lý ngày 16/4/2021.
2	CVE-2021-34523	- **Mô tả:** Lỗ hổng tồn tại trong Microsoft Exchange Server, cho phép đối tượng tấn công thực thi mã từ xa. - **Điểm CVSS:** 9.1 (cao) - **Ảnh hưởng:** Exchange Server 2019/2016/2013 - **Nguồn tham khảo:** https://msrc.microsoft.com/update-	Lỗ hổng mới công bố ngày 13/7/2021.

		guide/vulnerability/CVE-2021-34523	
3	CVE-2021-34527	- **Mô tả:** Lỗ hổng tồn tại trong Windows Print Spooler, cho phép đối tượng tấn công thực thi mã từ xa. - **Điểm CVSS:** 8.8 (cao) - **Nguồn tham khảo:** https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527	- Công văn số 2210/BTTTT-CATTT về việc dự báo sớm nguy cơ tấn công mạng trên diện rộng ngày 22/6/2021. - Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin, Bộ Thông tin và truyền thông đã có cảnh báo rộng rãi gửi trực tiếp đến các cơ quan tổ chức thông qua thư điện tử, Page FB chính thức của NCSC.
4	CVE-2021-33781	- **Mô tả:** Lỗ hổng cho phép đối tượng có đặc quyền thấp tấn công từ xa vượt qua các cơ chế kiểm tra bảo mật trong dịch vụ Active Directory để đạt được các đặc quyền cao hơn trên máy mục tiêu. - **Điểm CVSS:** 8.1 (cao) - **Ảnh hưởng:** Windows 10, Windows Server 2019. - **Nguồn tham khảo:** https://msrc.microsoft.com/update-	Lỗ hổng mới công bố ngày 13/7/2021.

		guide/vulnerability/CVE-2021-33781	
5	CVE-2021-34492	- **Mô tả:** Lỗ hổng cho phép đối tượng tấn công vượt qua cơ chế kiểm tra trong Windows Certificate để giả mạo chứng chỉ. - **Điểm CVSS:** 8.1 (cao) - **Ảnh hưởng:** Windows 10/8.1/RT8.1/7, Windows Server 2016/2012/2008. - **Nguồn tham khảo:** https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34492	Lỗ hổng mới công bố ngày 13/7/2021.

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 7 của Microsoft:

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

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

- Đánh giá của Zero Day Initiative:

https://zerodayinitiative.com/blog/2021/7/13/the-july-2021-security-update-review