

Phụ lục 2
THÔNG TIN VỀ CÁC LỖ HỔNG AN TOÀN THÔNG TIN
TRONG SẢN PHẨM MICROSOFT THÁNG 01/2024
(Kèm theo Văn bản số /STTTT-CĐS ngày / /2024
của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hổng an toàn thông tin

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-20674	<ul style="list-style-type: none">- Điểm: CVSS: 9.0 (Nghiêm trọng)- Mô tả: Lỗ hổng trong Windows Kerberos cho phép đối tượng tấn công vượt qua cơ chế bảo vệ để thực hiện tấn công giả mạo.- Ảnh hưởng: Windows 10, Windows 11; Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20674
2	CVE-2024-21318	<ul style="list-style-type: none">- Điểm: CVSS: 8.8 (Cao)- Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.- Ảnh hưởng: Microsoft SharePoint Server 2016, 2019; Microsoft SharePoint Server Subscription Edition.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21318
3	CVE-2024-20677	<ul style="list-style-type: none">- Điểm: CVSS: 7.8 (Cao)- Mô tả: Lỗ hổng trong Microsoft Office cho	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20677

		phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office 2019; Microsoft Office LTSC; Microsoft 365 Apps.	
4	CVE-2024-20700	- Điểm: CVSS: 7.5 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20700

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/2024/1/9/the-january-2024-security-update-review>