

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT
TRONG SẢN PHẨM MICROSOFT

*(Kèm theo Công văn số /CATTT-NCSC ngày / /2022
của Cục An toàn thông tin)*

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-37969	<ul style="list-style-type: none"> - Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Windows Common Log File System Driver cho phép đối tượng tấn công thực thi mã từ xa với các đặc quyền nâng cao. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37969
2	CVE-2022-34718	<ul style="list-style-type: none"> - Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows TCP/IP cho phép đối tượng tấn công chưa xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34718
3	CVE-2022-34724	<ul style="list-style-type: none"> - Điểm CVSS: 7.5 (Cao) - Lỗ hổng trong Windows DNS Server cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34724
4	CVE-2022-3075	<ul style="list-style-type: none"> - Lỗ hổng trong Chromium cho phép đối tượng tấn công chưa xác 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3075

		<p>thực có thể thực thi mã từ xa.</p> <ul style="list-style-type: none"> - Ảnh hưởng: Microsoft Edge (Chromium-based) 	
5	CVE-2022-34721, CVE-2022-34722	<ul style="list-style-type: none"> - Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows Internet Key Exchange (IKE) Protocol Extensions cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022. 	<p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34721</p> <p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34722</p>
6	CVE-2022-37961 CVE-2022-35823 CVE-2022-38008 CVE-2022-38009	<ul style="list-style-type: none"> - Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SherePoint Foundation 2013, SharePoint Server 2013/2016/2019, Microsoft SharePoint Enterprise Server 2013. 	<p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37961</p> <p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35823</p> <p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38008</p> <p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38009</p>
7	CVE-2022-37962	<ul style="list-style-type: none"> - Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft PowerPoint cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office 2013/2016/2019, Office 365 Apps, Office LTSC 2021. 	<p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37962</p>

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. Tài liệu tham khảo

<https://msrc.microsoft.com/update-guide/releaseNote/2022-Sep>

<https://www.zerodayinitiative.com/blog/2022/9/13/the-september-2022-security-update-review>