

Phụ lục: Thông tin các lỗ hổng bảo mật

(Kèm theo công văn số /UBND-VHTT ngày tháng năm 2022 của UBND huyện)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-34713	<ul style="list-style-type: none">- Điểm CVSS: 7.8 (Cao)- Lỗ hổng trong Microsoft Windows Support Diagnostic Tool (MSDT) cho phép đối tượng tấn công thực thi mã từ xa.- Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34713
2	CVE-2022-21980 CVE-2022-24477 CVE-2022-24516 CVE-2022-30134	<ul style="list-style-type: none">- Điểm CVSS: 8.0 (Cao)- Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thu thập thông tin và thực hiện leo thang đặc quyền.- Ảnh hưởng: Microsoft Exchange Server 2013/2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21980 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24477 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24516 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30134
3	CVE-2022-35804	<ul style="list-style-type: none">- Điểm CVSS: 8.8 (Cao)- Lỗ hổng trong SMB Client and Server cho phép đối tượng tấn công chưa xác thực có thể thực thi mã từ xa.- Ảnh hưởng: Windows 11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35804
4	CVE-2022-34715	<ul style="list-style-type: none">- Điểm CVSS: 9.8 (Nghiêm trọng)- Lỗ hổng trong Windows Network File System cho phép đối tượng tấn công chưa xác thực có thể thực thi mã từ xa.- Ảnh hưởng: Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34715

5	CVE-2022-35742	<ul style="list-style-type: none"> - Điểm CVSS: 7.5 (Cao) - Lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ. - Ảnh hưởng: Microsoft Outlook 2012/2016, Microsoft Office LTSC 2021/2019, Microsoft 365 Apps. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35742
---	----------------	---	---

2. Hướng dẫn khắc phục

Hướng dẫn chi tiết khắc phục các lỗ hổng bảo mật trên tại địa chỉ: <https://attt.thanhhoa.gov.vn> (Mục Hướng dẫn → Kỹ năng An toàn thông tin)

The image shows a screenshot of the website 'TRUNG TÂM ĐIỀU HÀNH AN TOÀN AN NINH MẠNG TỈNH THANH HÓA'. The navigation menu at the top includes 'Trang chủ', 'Tin tức', 'Cảnh báo', 'Hướng dẫn', and 'Hỗ trợ'. The 'Hướng dẫn' menu item is highlighted with a red box, and a dropdown menu is open, showing 'Kỹ năng an toàn thông tin', 'Công cụ', and 'Video'. Below the navigation menu, there is a blue banner with the text 'Dự báo sớm nguy cơ tấn công mạng trên diện rộng'. The banner contains a paragraph of text and a red button that says 'BẤM VÀO ĐÂY ĐỂ XEM CHI TIẾT'.

3. Tài liệu tham khảo

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

<https://www.zerodayinitiative.com/blog/2022/8/9/the-august-2022-security-update-review>