

**Phụ lục:** Thông tin các lỗ hổng bảo mật  
(Kèm theo công văn số /UBND-VHTT ngày tháng 5 năm 2022 của  
UBND huyện Cẩm Thủy)

---

**1. Thông tin các lỗ hổng bảo mật**

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-26925	<ul style="list-style-type: none"><li>- Điểm CVSS: 9.8 (Nghiêm trọng)</li><li>- Lỗ hổng trong Windows LSA cho phép đối tượng tấn công không cần xác thực có thể thực hiện tấn công giả mạo (spoofing) kết hợp với NTLM relay attack từ đó nâng cao đặc quyền trong hệ thống mục tiêu.</li><li>- Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2022/2019/2016/2012/2008</li></ul>	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-26925">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-26925</a>
2	CVE-2022-26923	<ul style="list-style-type: none"><li>- Điểm CVSS: 8.8 (Cao)</li><li>- Lỗ hổng trong Active Directory Domain Services cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.</li><li>- Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019/2022.</li></ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24491">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24491</a>
3	CVE-2022-26937	<ul style="list-style-type: none"><li>- Điểm CVSS: 9.8 (Nghiêm trọng)</li><li>- Lỗ hổng trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa.</li></ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26937">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26937</a>

		<ul style="list-style-type: none"> <li>- Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022.</li> </ul>	
4	CVE-2022-29972	<ul style="list-style-type: none"> <li>- Lỗ hổng trong Magnitude Simba Amazon Redshift ODBC Driver cho phép đối tượng thực thi mã từ xa.</li> </ul>	<p><a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29972">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29972</a></p> <p><a href="https://msrc-blog.microsoft.com/2022/05/09/vulnerability-mitigated-in-the-third-party-data-connector-used-in-azure-synapse-pipelines-and-azure-data-factory-cve-2022-29972">https://msrc-blog.microsoft.com/2022/05/09/vulnerability-mitigated-in-the-third-party-data-connector-used-in-azure-synapse-pipelines-and-azure-data-factory-cve-2022-29972</a></p>
5	CVE-2022-21978	<ul style="list-style-type: none"> <li>- Điểm CVSS: 8.2 (Cao)</li> <li>- Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.</li> <li>- Ảnh hưởng: Windows Server 2013/2016/2019.</li> </ul>	<p><a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21978">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21978</a></p>
6	CVE-2022-22017	<ul style="list-style-type: none"> <li>- Điểm CVSS: 8.8 (Cao)</li> <li>- Lỗ hổng trong Remote Desktop Protocol Client cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Windows 11, Windows Server 2022.</li> </ul>	<p><a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22017">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22017</a></p>
7	CVE-2022-29110	<ul style="list-style-type: none"> <li>- Điểm CVSS: 7.8 (Cao)</li> <li>- Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.</li> </ul>	<p><a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29110">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29110</a></p>

		- Ảnh hưởng: Microsoft Office Web Apps Server 2013, Microsoft Excel 2013/2016.	
8	CVE-2022-29108	- 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 SharePoint Server 2016/2019, Microsoft SharePoint Foundation 2013.	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29108">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29108</a>

## 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 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 visible below it, containing 'Kỹ năng an toàn thông tin', 'Công cụ', and 'Video'. The main content area features a blue background with a server rack and a laptop, and a headline: 'Dự báo sớm nguy cơ tấn công mạng trên diện rộng'. Below the headline is 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-May>

<https://www.zerodayinitiative.com/blog/2022/5/10/the-may-2022-security-update-review>