

Số: /CATT-NCSC  
V/v lỗ hổng bảo mật ảnh hưởng Cao và  
Nghiêm trọng trong các sản phẩm  
Microsoft công bố tháng 5/2022

Hà Nội, ngày tháng năm 2022

Kính gửi:

- Đơn vị chuyên trách về CNTT các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước; các Ngân hàng TMCP; các tổ chức tài chính;
- Hệ thống các đơn vị chuyên trách về an toàn thông tin.

Ngày 10/5/2022, Microsoft đã phát hành danh sách bản vá tháng 5 với 74 lỗ hổng bảo mật trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý các lỗ hổng bảo mật sau:

Các lỗ hổng bảo mật có mức ảnh hưởng Nghiêm trọng:

- Lỗ hổng bảo mật **CVE-2022-26925** trong Windows LSA cho phép đối tượng tấn công không cần xác thực có thể thực hiện tấn công giả mạo (spoofing). Trong thực tế, lỗ hổng này đang được sử dụng kết hợp với NTLM relay attack, từ đó giúp đối tượng tấn công nâng cao đặc quyền trong hệ thống mục tiêu.

- Lỗ hổng bảo mật **CVE-2022-26937** trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-29972** trong Magnitude Simba Amazon Redshift ODBC Driver cho phép đối tượng thực thi mã từ xa.

Các lỗ hổng bảo mật có mức ảnh hưởng Cao:

- Lỗ hổng bảo mật **CVE-2022-26923** trong Active Directory Domain Services cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-21978** trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-22017** trong Remote Desktop Protocol Client cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-29110** trong Microsoft Excel cho phép đối

tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-29108** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

*Thông tin chi tiết các lỗ hổng bảo mật có tại phụ lục kèm theo.*

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Cục An toàn thông tin khuyến nghị Quý đơn vị thực hiện:

1. Kiểm tra, rà soát, xác định máy sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công (tham khảo thông tin tại phụ lục kèm theo).

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

3. Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: [ais@mic.gov.vn](mailto:ais@mic.gov.vn).

Trân trọng./.

**Nơi nhận:**

- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Huy Dũng (để b/c);
- Cục A05, Bộ Công an;
- Bộ Tư lệnh 86, Bộ Quốc phòng;
- Ban Cơ yếu Chính phủ;
- Cục trưởng;
- Trung tâm VNCERT/CC, phòng ATHTTT;
- Lưu: VT, NCSC.

**CỤC TRƯỞNG**

**Nguyễn Thành Phúc**

**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**

<b>STT</b>	<b>CVE</b>	<b>Mô tả</b>	<b>Link tham khảo</b>
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><li>- Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022.</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>

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> <li>- Ảnh hưởng: Microsoft Office Web Apps Server 2013, Microsoft Excel 2013/2016.</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>
8	CVE-2022-29108	<ul style="list-style-type: none"> <li>- Điểm CVSS: 7.8 (Cao)</li> <li>- Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Microsoft SharePoint Server 2016/2019, Microsoft</li> </ul>	<p><a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29108">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29108</a></p>

		SharePoint Foundation 2013.	
--	--	--------------------------------	--

## **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-May>

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