SỞ THÔNG TIN VÀ TRUYỀN THÔNG THANH HÓA
**TRUNG TÂM CNTT&TT**

Số: 54 /TTCNTT&TT-QTHT
V/v lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 5/2022

**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM**
**Độc lập - Tự do - Hạnh phúc**

*Thanh Hoá, ngày 12 tháng5 năm 2022*

Kính gửi:
- Văn Phòng Tỉnh ủy;
- Văn Phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn Phòng UBND tỉnh;
- Các sở, ban, ngành cấp tỉnh;
- UBND các huyện, thị xã, thành phố;
- Các tổ chức đoàn thể chính trị cấp tỉnh;
- Các doanh nghiệp viễn thông, CNTT trên địa bàn tỉnh.

Căn cứ Công văn số 674/CATTT-NCSC ngày 11/5/2022 về lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 5/2022 của Cục An toàn thông tin, Bộ Thông tin và Truyền thông. Theo đó, 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:

- 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. (*Chi tiết các lỗ hổng tại Phụ lục kèm theo*).

Để tăng cường chủ động phòng ngừa các rủi ro mất an toàn thông tin tại các hệ thống thông tin của các cơ quan, địa phương do hình thức tấn công trên có thể xảy ra, Trung tâm Công nghệ thông tin và Truyền thông đề nghị các cơ quan, đơn vị chỉ đạo các bộ phận, cá nhân thực hiện những nội dung sau:

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. Hướng dẫn kỹ thuật cách thức thực hiện chi tiết đối với từng lỗ hổng bảo mật tại địa chỉ: https://attt.thanhhoa.gov.vn

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.

Trong quá trình thực hiện, nếu gặp khó khăn, vướng mắc về kỹ thuật liên quan đến các nội dung, công việc trên đề nghị liên hệ với Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa (cơ quan thường trực của Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh) để phối hợp hỗ trợ, xử lý.

Điện thoại: (0237)3718.699

Thư điện tử: ungcuusuco@thanhhoa.gov.vn

Xin trân trọng cảm ơn./.

***Nơi nhận:***
- Như kính gửi;
- Sở TT&TT (để b/c);
- PGĐ Sở Nguyễn Văn Tước (để b/c);
- Giám đốc Trung tâm (để b/c);
- Lưu: VT, QTHT.

**KT. GIÁM ĐỐC**
**PHÓ GIÁM ĐỐC**

SỞ THÔNG TIN VÀ TRUYỀN THÔNG TỈNH THANH HÓA
TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

**Trần Ngọc Hưng**

**Phụ lục**: Thông tin các lỗ hổng bảo mật

*(Kèm theo công văn số /TTCNTT&TT-QTHT ngày tháng năm 2022 của Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa)*

**1. Thông tin các lỗ hổng bảo mật**

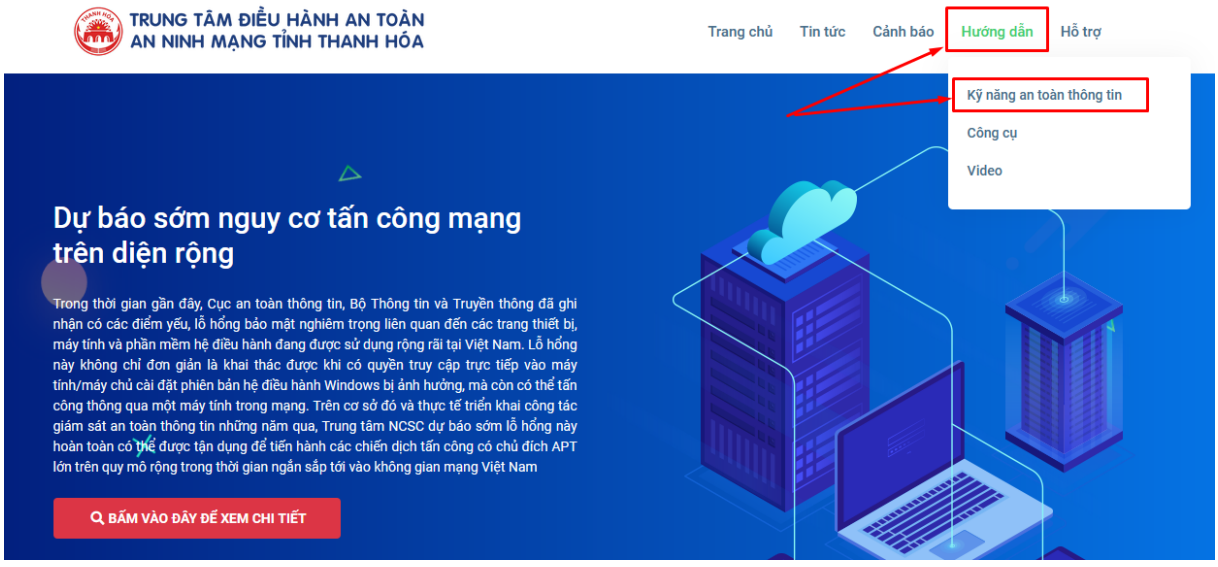
| STT | CVE | Mô tả | Link tham khảo |
|---|---|---|---|
| 1 | CVE-2022-26925 | - Điểm CVSS: 9.8 (Nghiêm trọng)<br>- Lỗ hổng trong Windows LSA cho phép đối tượng tấn công không cần xác thực có thể thực hiện tấn công giả mạo (spoofing) kết hợp với NTLM relay attack từ đó nâng cao đặc quyền trong hệ thống mục tiêu.<br>- Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2022/2019/2016/2012/2008. | https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-26925 |
| 2 | CVE-2022-26923 | - Điểm CVSS: 8.8 (Cao)<br>- Lỗ hổng trong Active Directory Domain Services cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.<br>- Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019/2022. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24491 |
| 3 | CVE-2022-26937 | - Điểm CVSS: 9.8 (Nghiêm trọng)<br>- Lỗ hổng trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26937 |

| | | | |
|---|---|---|---|
| | | - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022 . | |
| 4 | CVE-2022-29972 | - Lỗ hổng trong Magnitude Simba Amazon Redshift ODBC Driver cho phép đối tượng thực thi mã từ xa. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29972<br><br>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 |
| 5 | CVE-2022-21978 | - Điểm CVSS: 8.2 (Cao)<br><br>- Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.<br><br>- Ảnh hưởng: Windows Server 2013/2016/2019. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21978 |
| 6 | CVE-2022-22017 | - Điểm CVSS: 8.8 (Cao)<br><br>- Lỗ hổng trong Remote Desktop Protocol Client cho phép đối tượng tấn công thực thi mã từ xa.<br><br>- Ảnh hưởng: Windows 11, Windows Server 2022. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22017 |
| 7 | CVE-2022-29110 | - Điểm CVSS: 7.8 (Cao)<br><br>- Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29110 |

| | | | |
|---|---|---|---|
| | | - Ảnh hưởng: Microsoft Office Web Apps Server 2013, Microsoft Excel 2013/2016. | |
| 8 | CVE-2022-29108 | - Điểm CVSS: 7.8 (Cao)<br>- Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Microsoft SharePoint Server 2016/2019, Microsoft SharePoint Foundation 2013. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29108 |

## 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*)




## 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