UBND TỈNH NINH THUẬN
**SỞ Y TẾ**
Số: 3101 /SYT-KHNVTC

V/v lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 7/2024.

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

*Ninh Thuận, ngày 17 tháng 7 năm 2024*

Kính gửi: Các đơn vị trực thuộc.

Tiếp nhận Công văn số 2005/STTTT-TTCNTTTT ngày 15/7/2024 của Sở Thông tin và Truyền thông về lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 7/2024.

Ngày 09/07/2024, Microsoft đã phát hành danh sách bản vá tháng 07 với 139 lỗ hổng an toàn thông tin trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý vào các lỗ hổng an toàn thông tin có mức ảnh hưởng cao và nghiêm trọng sau: *(1)* 03 lỗ hổng an toàn thông tin CVE-2024-38074, CVE-2024-38076, CVE-2024-38077 trong Windows Remote Desktop Licensing Service cho phép đối tượng tấn công thực thi mã từ xa; *(2)* Lỗ hổng an toàn thông tin CVE-2024-38060 trong Windows Imaging Component cho phép đối tượng tấn công thực thi mã từ xa; *(3)* 03 lỗ hổng an toàn thông tin CVE-2024-38023, CVE-2024-38024, CVE-2024-38094 trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa; *(4)* Lỗ hổng an toàn thông tin CVE-2024-38021 trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa; *(5)* Lỗ hổng an toàn thông tin CVE-2024-38080 trong Windows Hyper-V cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế; *(6)* Lỗ hổng an toàn thông tin CVE-2024-38112 trong Windows MSHTML Platform cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). Lỗ hổng hiện đang bị khai thác trong thực tế.

*(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 các đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Y tế yêu cầu các 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 được hỗ trợ các đơn vị liên hệ Trung tâm Giám sát an toàn, an ninh, thông tin mạng *(qua tổng đài điện thoại 1022 hoặc thư điện tử: ioc@ninhthuan.gov.vn)*.

Sở Y tế thông báo và yêu cầu các đơn vị triển khai thực hiện./.

***Nơi nhận:***
- Như trên;
- Lãnh đạo Sở;
- Website Sở Y tế;
- Lưu: VT, KHNVTC.

**KT. GIÁM ĐỐC**
**PHÓ GIÁM ĐỐC**

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ Y TẾ
TỈNH NINH THUẬN

**Bùi Văn Kỳ**

**Phụ lục**
**THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG SẢN PHẨM MICROSOFT**
*(Kèm theo Công văn số /SYT-KHNVTC ngày / /2024 của Sở Y tế)*

## 1. Thông tin các lỗ hổng bảo mật

| STT | CVE | Mô tả | Link tham khảo |
|---|---|---|---|
| 1 | CVE-2024-38074<br>CVE-2024-38076<br>CVE-2024-38077 | - Điểm CVSS: 9.8 (Nghiêm trọng)<br>- Mô tả: Lỗ hổng trong Windows Remote Desktop Licensing Service cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Windows Server 2008, 2012, 2016, 2019, 2022. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38074<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38076<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38077 |
| 2 | CVE-2024-38060 | - Điểm CVSS: 8.8 (Nghiêm trọng)<br>- Mô tả: Lỗ hổng trong Windows Imaging Component cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38060 |
| 3 | CVE-2024-38023<br>CVE-2024-38024<br>CVE-2024-38094 | - Điểm CVSS: 7.2 (Nghiêm trọng)<br>- Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38023<br>https://msrc.microsoft.com/update- |

| | | | |
|---|---|---|---|
| | | mã từ xa.<br>- Ảnh hưởng: Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, Microsoft SharePoint Server Subscription Edition. | guide/vulnerability/CVE-2024-38024<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38094 |
| 4 | CVE-2024-38021 | - Điểm CVSS: 8.8 (Cao)<br>- Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Microsoft Office 2016, 2019, Microsoft Office LTSC 2021, Microsoft 365 Apps for Enterprise. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38021 |
| 5 | CVE-2024-38080 | - Điểm CVSS: 7.8 (Cao)<br>- Mô tả: Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.<br>- Ảnh hưởng: Windows 11, Windows Server 2022. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38080 |
| 6 | CVE-2024-38112 | - Điểm CVSS: 7.5 (Cao)<br>- Mô tả: Lỗ hổng trong Windows MSHTML Platform cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). Lỗ hổng hiện | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112 |

| | | | |
|---|---|---|---|
| | | đang bị khai thác trong thực tế.<br>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022. | |

**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/

https://www.zerodayinitiative.com/blog/2024/7/9/the-july-2024-security-update-review