UBND TỈNH ĐỒNG NAI
**SỞ Y TẾ**

Số: 4701 /SYT-VP

V/v lỗ hổng bảo mật ảnh hưởng trong các sản phẩm Microsoft công bố tháng 6/2022.

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

*Đồng Nai, ngày 06 tháng 07 năm 2022*

Kính gửi: Các đơn vị trực thuộc Sở Y Tế.

Căn cứ Công văn số 1488/STTTT-CNTTVT ngày 23/06/2022 của Sở Thông tin và Truyền thông về việc lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 6/2022.

Sở Y tế thông báo tình hình trên đến các đơn vị trực thuộc để có hướng xử lý thích hợp đối với các sản phẩm Microsoft hiện đang sử dụng tại đơn vị.

*(Đính kèm Công văn số 1488/STTTT-CNTTVT ngày 23/06/2022).*

Do sự việc có ảnh hưởng cao và nghiêm trọng, đề nghị các đơn vị khẩn trương thực hiện theo hướng dẫn của công văn đính kèm.

Trân trọng./.

***Nơi nhận:***
- Như trên;
- Lưu: VT, VP.

**KT.GIÁM ĐỐC**
**PHÓ GIÁM ĐỐC**

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ Y TẾ
TỈNH ĐỒNG NAI

**Nguyễn Hữu Tài**

Số 2 - Phan Đình Phùng, phường Quang Vinh, thành phố Biên Hoà, tỉnh Đồng Nai
ĐT: (02513) 942641, Fax: (02513) 847269, Email: syt@dongnai.gov.vn, Website: syt.dongnai.gov.vn

UBND TỈNH ĐỒNG NAI
**SỞ THÔNG TIN VÀ TRUYỀN THÔNG**

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

Số: 1488 /STTTT-CNTTVT
V/v lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 6/2022

*Đồng Nai, ngày 23 tháng 6 năm 2022*

Kính gửi:
- Các cơ quan đảng, nhà nước trên địa bàn tỉnh;
- Các tổ chức chính trị - xã hội thuộc địa bàn tỉnh;
- Viettel Đồng Nai, VNPT Đồng Nai, Mobifone Đồng Nai;
- Trung tâm Công nghệ thông tin tỉnh Đồng Nai.

Sở Thông tin và Truyền thông nhận văn bản 869/CATTT-NCSC ngày 16/6/2022 của Cục An toàn thông tin về việc lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 6/2022;

Theo văn bản trên, ngày 14/6/2022 Microsoft đã phát hành danh sách bản vá tháng 6 với 55 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-2022-30190** (hay còn gọi là Follina) trong Windows Microsoft Support Diagnotic Tool (MSDT) cho phép đối tượng tấn công thực thi mã tùy ý. Mặc dù, có điểm CVSS: 7.8 (Cao) nhưng mã khai thác của lỗ hổng này đã được công bố rộng rãi trên Internet, đặc biệt đang được các nhóm tấn công khai thác triệt để. Các cơ quan, tổ chức cần tiến hành cập nhật bản vá hoặc triển khai các biện pháp hạn chế ngay khi có thể để tránh nguy cơ bị tấn công thông qua lỗ hổng này.

Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin cũng đã cảnh báo rộng rãi về lỗ hổng Follina tại văn bản số **786/CATTT-NCSC** về việc lỗ hổng bảo mật CVE-2022-30190 trong Microsoft Support Diagnostic Tool phát hành ngày 01/6/2022.

- Lỗ hổng bảo mật **CVE-2022-30136** trong Windows Network File System cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa.

Các lỗ hổng bảo mật có mức ảnh hưởng Cao:

- Lỗ hổng bảo mật **CVE-2022-30163** trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-30139** trong Windows Lightweight Directory Access Protocol (LDAP) cho phép đối tượng tấn công thực thi mã từ xa.

- 02 lỗ hổng bảo mật **CVE-2022-30157, CVE-2022-30158** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

Số 01, đường 30/4, phường Thanh Bình, TP. Biên Hòa, tỉnh Đồng Nai.
ĐT: (0251) 3810.269 – https://stttt.dongnai.gov.vn

- Lỗ hổng bảo mật **CVE-2022-30165** trong Windows Kerberos cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-30173** Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-30174** trong Microsoft Office 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.*

Để tăng cường đảm bảo an toàn thông tin mạng trên địa bàn tỉnh, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông đề nghị Quý đơn vị chủ động thực hiện các biện pháp 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 (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 hoặc Sở Thông tin và Truyền thông, điện thoại 0251.3810.269, thư điện tử: attt@dongnai.gov.vn.

Trân trọng./.

***Nơi nhận:***
- Như trên;
- UBND tỉnh (b/c);
- Giám đốc và Phó Giám đốc Sở;
- Lưu: VT, CNTTVT, Thịnh.

**KT. GIÁM ĐỐC**
**PHÓ GIÁM ĐỐC**

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH ĐỒNG NAI

**Võ Hoàng Khai**

**Phụ lục**

**THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG SẢN PHẨM MICROSOFT**

*(Kèm theo văn bản số 1488 /STTTT-CNTTVT ngày 23 / 6/2022 của Sở Thông tin và Truyền thông)*

**1. Thông tin các lỗ hổng bảo mật**

| STT | CVE | Mô tả | Link tham khảo |
|---|---|---|---|
| 1 | CVE-2022-30190 (Follina) | - Điểm CVSS: 7.8 (Cao)<br>- Lỗ hổng trong Windows Microsoft Support Diagnotic Tool (MSDT) cho phép đối tượng tấn công thực thi mã tùy ý.<br>- Ảnh hưởng: Windows 7/8.1/10, Windows Server 2008/2012/2016. | https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190<br>Văn bản số 786/CATTT-NCSC về việc lỗ hổng bảo mật CVE-2022-30190 trong Microsoft Support Diagnostic Tool phát hành ngày 01/6/2022. |
| 2 | CVE-2022-30136 | - Điểm CVSS: 9.8 (Nghiêm trọng)<br>- Lỗ trong Windows Network File System cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa.<br>- Ảnh hưởng: Windows Server 2012/2016/2019. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30136 |
| 3 | CVE-2022-30163 | - Điểm CVSS: 8.5 (Cao)<br>- Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Windows 8.1/10/11, Windows Server 2008/2012/2016. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30163 |

| | | | |
|---|---|---|---|
| 4 | CVE-2022-30139 | - Điểm CVSS:7.5 (cao)<br>- Lỗ hổng trong Windows Lightweight Directory Access Protocol (LDAP) cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Windows 10, Windows Server 2016/2019/2022. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30139 |
| 5 | CVE-2022-30157<br>CVE-2022-30158 | - Điểm CVSS: 8.8 (Cao)<br>- Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: SharePoint Server 2019, SharePoint Enterprise Server 2016. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30157<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30158 |
| 6 | CVE-2022-30165 | - Điểm CVSS: 8.8 (Cao)<br>- Lỗ hổng trong Windows Kerberos cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.<br>- Ảnh hưởng: Windows 10/11, Windows Server 2016/2022. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30165 |
| 7 | CVE-2022-30173 | - Điểm CVSS: 7.8 (Cao)<br>- Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Excel 2013/2016. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30173 |
| 8 | CVE-2022-30174 | - Điểm CVSS: 7.4 (Cao)<br>- Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Microsoft 365 Apps, Microsoft Office LTSC 2021. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30174 |

**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-Jun

https://www.zerodayinitiative.com/blog/2022/6/14/the-june-2022-security-update-review