| | |
|---|---|
| **UỶ BAN NHÂN DÂN**<br>**THÀNH PHỐ BẮC NINH** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**<br>**Độc lập - Tự do - Hạnh phúc** |
| Số: 1373 /UBND- VHTT<br>V/v cảnh báo, phát hiện, xử lý đảm bảo an toàn thông tin, lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 6/2022 | *Thành phố Bắc Ninh, ngày 22 tháng 6 năm 2022* |

Kính gửi:
- Các cơ quan, đơn vị thuộc UBND thành phố;
- UBND các phường trên địa bàn thành phố.

Thực hiện Công văn số 431/STTTT- CNTT ngày 20/6/2022 của Sở Thông tin và Truyền thông tỉnh Bắc Ninh về việc lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 6/2022;

Tại công văn số 869/CATTT-NCSC ngày 16/6/2022 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông đã thông báo phát hành danh sách bản vá tháng 6 với 55 lỗ hổng bảo mật có mức ảnh hưởng cao và nghiêm trọng trong các sản phẩm của Microsoft, cụ thể như sau:

**1. 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.

UBND thành phố cũng đã cảnh báo rộng rãi về lỗ hổng Follina tại văn bản số 1312/UBND- VHTT ngày 14/6/2022 về cảnh báo, xử lý lỗ hổng bảo mật CVE-2022- 30190 trong Microsoft Support Diagnostic Tool.

- 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.

**2. 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.

- 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.

*(Có Phụ lục thông tin chi tiết về các lỗ hổng bảo mật gửi kèm)*

Để đảm bảo kịp thời xử lý, khắc phục các lỗ hổng bảo mật về an toàn thông tin cho hệ thống thông tin của các cơ quan, đơn vị và UBND các phường trên địa bàn thành phố Bắc Ninh (nếu có).

UBND thành phố yêu cầu các cơ quan, đơn vị và UBND các phường triển khai thực hiện tốt một số nhiệm vụ 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.

*(Thực hiện theo 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 về an toàn thông tin nhằm phát hiện và xử lý kịp thời các nguy cơ tấn công mạng.

**3.** Ngay khi phát hiện sự cố, nếu các cơ quan đơn vị và UBND các phường không có khả năng xử lý yêu cầu thông báo về đầu mối Trung tâm Công nghệ Thông tin và Truyền thông - Sở Thông tin và Truyền thông tỉnh Bắc Ninh để được hỗ trợ xử lý, khắc phục kịp thời.

- Đồng chí: Lại Hữu Dương - Phó Giám đốc Trung tâm CNTT&TT, số điện thoại 0913.629.199.

- Đồng chí: Nguyễn Thế Thủy - Phòng Quản trị và Tích hợp hệ thống - Trung tâm CNTT&TT, số điện thoại 0222.3875606 hoặc 0929003888.

- Địa chỉ thư điện tử pqtthht.stttt@bacninh.gov.vn.

Yêu cầu các cơ quan, đơn vị và UBND các phường nghiêm túc triển khai thực hiện./.

***Nơi nhận:***
- Như kính gửi (t/h);
- TT Thành ủy - HĐND thành phố (b/c);
- Chủ tịch, các PCT UBND thành phố;
- Lưu: VT, VHTT.

**KT. CHỦ TỊCH**
**PHÓ CHỦ TỊCH**

**Nguyễn Mạnh Hiếu**

# PHỤ LỤC
## Thông tin về các lỗ hổng bảo mật trong sản phẩm Microsoft
*(Kèm theo Công văn số 1373 /UBND-VHTT ngày 22 /6/2022 của UBND thành phố Bắc Ninh)*

### 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/updateguide/enUS/vulnerability/CVE2022-30190<br>Công văn số 1312/UBND- VHTT ngày 14/6/2022 của UBND thành phố Bắc Ninh về cảnh báo, xử lý lỗ hổng bảo mật CVE-2022-30190 trong Microsoft Support Diagnostic Tool. |
| 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/updateguide/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/updateguide/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/updateguide/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/updateguide/vulnerability/CVE-2022-30157<br>https://msrc.microsoft.com/updateguide/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/updateguide/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/updateguide/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/updateguide/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, các cơ quan, đơn vị tham khảo 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*