UBND THÀNH PHỐ BẮC KẠN
PHÒNG VĂN HÓA VÀ THÔNG TIN

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

Số:137 /CV-VHTT
V/v thông báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 7/2022

TP. Bắc Kạn, ngày 20 tháng 7 năm 2022

Kính gửi:
- Ủy ban MTTQ và các đoàn thể thành phố;
- Các phòng, ban, đơn vị thành phố;
- Ủy ban nhân dân xã, phường.

Thực hiện Công văn số 828/STTTT-CNTT-BCVT ngày 18 tháng 7 năm 2022 của Sở Thông tin và Truyền thông tỉnh Bắc Kạn về việc thông báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 7/2022. Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các phòng, ban, ngành, đoàn thể, Uỷ ban nhân dân xã, phường, Phòng Văn hoá và Thông tin thành phố Bắc Kạn thông báo các lỗ hổng bảo mật để các đơn vị biết, triển khai thực hiện các giải pháp về an toàn tthông tin với nội dung như sau:

1. Đối với 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. Đề nghị các cơ quan, đơn vị cần tiến hành cập nhật bản vá hoặc triển khai các biện pháp hạn chế ngay 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 ban 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.

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.

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

3. Đề nghị các cơ quan, đơn vị thực hiện một số biện pháp đảm bảo an toàn thông tin như sau:

- 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).*

- 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 phát hiện hoặc khó khăn, vướng mắc về thông tin lỗ hổng bảo mật đề nghị các cơ quan, đơn vị liên hệ Ủy ban nhân dân thành phố Bắc Kạn qua phòng Văn hóa và Thông tin *(bà Lâm Thị Trang, điện thoại 0969155599)* hoặc Sở thông tin và Truyền thông *(phòng Công nghệ thông tin, điện thoại: 0209 3871 626 hoặc ông Nguyễn Văn Cương, điện thoại 0989 332 044)* để phối hợp giải quyết.

Với nội dung trên đề nghị các cơ quan, đơn vị triển khai thực hiện./.

Nơi nhận:
Gửi bản điện tử:
- Như trên;
- CT, PCT UBND TP (B. Huế);
- Lưu: VHTT.

TRƯỞNG PHÒNG

CỘNG HÒA X.H.C.N VIỆT NAM
PHÒNG VĂN HÓA VÀ THÔNG TIN
TP. BẮC KẠN T. BẮC KẠN

Nông Ngọc Khanh

PHỤ LỤC
Thông tin về các lỗ hổng bảo mật trong sản phẩm Microsoft
(Kèm theo Công văn số 137 /CV-VHTT ngày 10/6/2022 của Phòng văn hoá và Thông tin thành phố Bắc Kạn)

1. Thông tin các lỗ hổng bảo mật

TT	CVE	Mô tả	Link tham khảo
1	CVE-2022-30190 (Follina)	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Windows Microsoft Support Diagnotic Tool (MSDT) cho phép đối tượng tấn công thực thi mã tùy ý. - Ảnh hưởng: Windows 7/8.1/10, Windows Server 2008/2012/2016.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190 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) - Lỗ trong Windows Network File System cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa. - 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) - Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa. - 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) - Lỗ hổng trong Windows Lightweight Directory Access	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30139

		Protocol (LDAP) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows Server 2016/2019/2022.	
5	CVE-2022-30157 CVE-2022-30158	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: SharePoint Server 2019, SharePoint Enterprise Server 2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30157 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30158
6	CVE-2022-30165	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Windows Kerberos cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - 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) - Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Excel 2013/2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30173
8	CVE-2022-30174	- Điểm CVSS: 7.4 (Cao) - Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - 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