

UBND TỈNH QUẢNG TRỊ
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: /STTTT-BCVT&CNTT
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng
cao và nghiêm trọng trong các sản phẩm
Microsoft công bố tháng 06/2022

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

Quảng Trị, ngày tháng 6 năm 2022

Kính gửi:

- Văn phòng UBND tỉnh;
- Các Sở, Ban, ngành cấp tỉnh;
- UBND các huyện, thị xã, thành phố.

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 Diagnostic 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.

- 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.

Thực hiện Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về Nâng cao năng lực phòng, chống phần mềm độc hại; Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam; Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 của Thủ tướng Chính phủ về việc ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng toàn quốc và Chương trình hành động số 161-CTHĐ/TU ngày 19/8/2019 của Ban Thường vụ Tỉnh ủy về việc thực hiện Nghị quyết số 30-NQ/TW ngày 25/7/2018 của Bộ Chính trị về Chiến lược An ninh mạng quốc gia; nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan, Sở Thông tin và Truyền thông đề nghị các cơ quan triển khai quyết liệt một số khuyến nghị 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.

Mọi vướng mắc vui lòng liên hệ: Sở Thông tin và Truyền thông - Thành viên mạng lưới Ứng cứu sự cố mạng Internet Việt Nam do Bộ Thông tin và Truyền thông thành lập. Đơn vị thường trực kỹ thuật: Trung tâm Công nghệ thông tin và Truyền thông, điện thoại 0233. 3898666./.

Nơi nhận:

- Như trên;
- Phòng PA05 - Công an tỉnh (p/h);
- Trung tâm CNTT-TT (t/h);
- Lưu: VT, BCVT&CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Nguyễn Thị Huyền

Phụ lục

Thông tin về các lỗ hổng bảo mật trong sản phẩm Microsoft

(Ban hành kèm theo văn bản số /STTTT-BCVT&CNTT ngày /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) - Lỗ hổng trong Windows Diagnostic 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 hổng 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.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30163

		- Ảnh hưởng: Windows 8.1/10/11, Windows Server 2008/2012/2016.	E-2022-30163
4	CVE-2022-30139	- Điểm CVSS:7.5 (cao) - Lỗ hổng trong Windows Lightweight Directory Access Protocol (LDAP) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows Server 2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30139
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>