

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

Hà Nội, ngày tháng năm 2022

Kính gửi:

- Đơn vị chuyên trách về CNTT các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước; các Ngân hàng TMCP; các tổ chức tài chính;
- Hệ thống các đơn vị chuyên trách về an toàn thông tin.

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.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Cục An toàn thông tin khuyến nghị Quý 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 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.

Trân trọng./.

Nơi nhận:

- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Huy Dũng (để b/c);
- Cục A05, Bộ Công an;
- Bộ Tư lệnh 86, Bộ Quốc phòng;
- Ban Cơ yếu Chính phủ;
- Cục trưởng;
- Trung tâm VNCERT/CC, phòng ATHTTT;
- Lưu: VT, NCSC.

CỤC TRƯỞNG

Nguyễn Thành Phúc

Phụ lục
Thông tin về các lỗ hổng bảo mật trong sản phẩm Microsoft
(Kèm theo Công văn số /CATT-NCSC ngày / /2022
của Cục An toàn thông tin)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-30190 (Follina)	<ul style="list-style-type: none">- Điểm CVSS: 7.8 (Cao)- Lỗ hổng trong Windows Microsoft Support 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.	<p>https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190</p> <p>Văn bản số 786/CATT-NCSC về việc lỗ hổng bảo mật CVE-2022-30190 trong Microsoft Support Diagnostic Tool phát hành ngày 01/6/2022.</p>
2	CVE-2022-30136	<ul style="list-style-type: none">- 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.	<p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30136</p>
3	CVE-2022-30163	<ul style="list-style-type: none">- 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.	<p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30163</p>
4	CVE-2022-30139	<ul style="list-style-type: none">- 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.	<p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30139</p>

5	CVE-2022-30157 CVE-2022-30158	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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>