

Số: /CATTT-NCSC
V/v lỗ hổng bảo mật ảnh hưởng cao và
nghiêm trọng trong các sản phẩm
Microsoft công bố tháng 01/2022

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 11/01/2022, Microsoft đã phát hành danh sách bản vá tháng 01 với 96 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:

1. Các lỗ hổng có mức ảnh hưởng Nghiêm trọng:

- Lỗ hổng bảo mật **CVE-2022-21907** trong HTTP Protocol Stack (<http.sys>) của Windows, cho phép đối tượng tấn công thực thi mã từ xa mà không cần xác thực.

2. Các lỗ hổng có mức ảnh hưởng Cao:

- 03 lỗ hổng bảo mật **CVE-2022-21846**, **CVE-2022-21969**, **CVE-2022-21855** trong Microsoft Exchange Server, cho phép đối tượng tấn công thực thi mã từ xa. Để khai thác lỗ hổng này, kẻ tấn công cần có quyền truy cập vào mạng mục tiêu từ đây có thể chiếm quyền điều khiển máy chủ.

- Lỗ hổng bảo mật **CVE-2022-21857** trong Active Directory, cho phép đối tượng nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-21840** trong Microsoft Office, cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-21911** trong .NET Framework, cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ.

- Lỗ hổng bảo mật **CVE-2022-21836** trong Windows Certificate, cho phép đối tượng tấn công giả mạo.

- Lỗ hổng bảo mật **CVE-2022-21841** trong Microsoft Excel, cho phép đối

tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-21837** trong Microsoft SharePoint Server, cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-21842** trong Microsoft Word, 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;
- Lưu: VT, NCSC.

CỤC TRƯỞNG

Nguyễn Thành Phúc

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỒNG BẢO MẬT TRONG MICROSOFT
(Kèm theo Công văn số /CATTT-NCSC ngày / /2022
của Cục An toàn thông tin)

1. Thông tin các lỗ hồng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-21907	<ul style="list-style-type: none">- Điểm CVSS: 9.8 (Nghiêm trọng)- Lỗ hồng trong HTTP Protocol, cho phép đối tượng tấn công thực thi mã từ xa.- Ảnh hưởng: Windows Server 2019/2022, Windows 11/10.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21907
2	CVE-2022-21846	<ul style="list-style-type: none">- Điểm CVSS: 9.0 (Cao)- Lỗ hồng trong Exchange Server, cho phép đối tượng tấn công thực thi mã từ xa.- Ảnh hưởng: Microsoft Exchange Server 2019/2016/2013.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21846
3	CVE-2022-21855	<ul style="list-style-type: none">- Điểm CVSS: 9.0 (Cao)- Lỗ hồng trong Exchange Server, cho phép đối tượng tấn công thực thi mã từ xa.- Ảnh hưởng: Microsoft Exchange Server 2019/2016/2013.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21855
4	CVE-2022-21969	<ul style="list-style-type: none">- Điểm CVSS: 9.0 (Cao)- Lỗ hồng trong Exchange Server, cho phép đối tượng tấn công thực thi mã từ xa.- Ảnh hưởng: Microsoft Exchange Server 2019/2016/2013.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21969
5	CVE-2022-21840	<ul style="list-style-type: none">- Điểm CVSS: 8.8 (Cao)- Lỗ hồng trong Microsoft Office, cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21840

		<ul style="list-style-type: none"> - Ảnh hưởng: Microsoft SharePoint Foundation 2013, SharePoint Server 2019, Microsoft Office 2016/2013/LTSC 2021/2019, Microsoft Excel 2016/2013, Microsoft 365 	
6	CVE-2022-21875	<ul style="list-style-type: none"> - Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Active Directory Domain Services, cho phép đối tượng tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2022/2019/2016/2012/2008, Windows 11/10/RT 8.1/7. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21857
7	CVE-2022-21911	<ul style="list-style-type: none"> - Điểm CVSS: 7.5 (Cao) - Lỗ hổng trong .NET Framework, cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ. - Ảnh hưởng: Microsoft .NET Framework 3.5 AND 4.7.2, 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2,... 	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21911
8	CVE-2022-21836	<ul style="list-style-type: none"> - Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Certificate, cho phép đối tượng tấn công thực hiện tấn công giả mạo - Ảnh hưởng: Windows Server 2022/2019/2016/2012/2008, Windows 10/RT 8.1/7. 	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21836

9	CVE-2022-21841	<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: Microsoft Office 2013/2016/2019/LTSC2021, Microsoft 365. 	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21841
10	CVE-2022-21837	<ul style="list-style-type: none"> - Điểm CVSS: 8.3 (cao) - Lỗ hổng trong Microsoft SharePoint Server, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server 2019, 2016 	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21837
11	CVE-2022-21842	<ul style="list-style-type: none"> - Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Microsoft Word, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Word 2016. 	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21842

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-Jan>
<https://msrc.microsoft.com/update-guide/en-us>