Báo cáo về các lỗ hổng an toàn thông tin trong các sản phẩm của Microsoft tháng 01/2025

1. Thông tin chung

Thực hiện chức năng quản lý nhà nước và tổ chức thực thi pháp luật về an toàn thông tin mạng, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin trong tháng vừa qua đã ghi nhận thông tin về các lỗ hổng an toàn thông tin của hãng Microsoft. Ngày 14/01/2025, Microsoft đã phát hành danh sách bản vá **tháng 01** với tổng **161 lỗ hổng an toàn thông tin** gồm có **159 lỗ hổng an toàn thông tin** trong các sản phẩm của hãng Microsoft và **02 lỗ hổng an toàn thông tin** trong các sản phẩm thuộc bên thứ ba có ảnh hưởng tới Microsoft, trong đó có 11 lỗ hổng mức Nghiêm trọng và 148 lỗ hổng mức độ Cao.

Các lỗ hổng này có mức độ ảnh hưởng **Cao** và **Nghiêm trọng**, có thể bị đối tượng tấn công khai thác để thực hiện các hành vi trái phép, gây ra nguy cơ mất an toàn thông tin và ảnh hưởng đến các hệ thống thông tin của cơ quan, tổ chức và doanh nghiệp.

Lỗ hổng an toàn thông tin tồn tại trên một số sản phẩm của Microsft như: Windows và các thành phần của Windows, Office và các thành phần của Office, Hyper-V, SharePoint Server, .NET và Visual Studio, Azure, BitLocker, Remote Desktop Services và Windows Virtual Trusted Platform Module.

*Thông tin chi tiết về lỗ hổng an toàn thông tin xem tại **mục 2** của báo cáo.*

Đề nghị các cơ quan, đơn vị, doanh nghiệp nghiên cứu thông tin về các lỗ hổng an toàn thông tin dưới đây, thực hiện rà soát hệ thống, xử lý các vấn đề về an toàn thông tin mạng trong hệ thống và gửi kết quả báo cáo rà soát về địa chỉ thư điện tử **ncsc@ais.gov.vn chậm nhất trước ngày 30 hàng tháng.**

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: ncsc@ais.gov.vn.

2. Thông tin chi tiết các lỗ hổng

Danh sách lỗ hổng an toàn thông tin đáng chú ý trong các sản phẩm của Microsoft tháng 01/2025

STT	CVE	Mô tả	Link tham khảo
1	CVE-2025-21333 CVE-2025-21334 CVE-2025-21335	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Windows Hyper-V NT Kernel Integration VSP cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2025.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21333 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21334 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21335
2	CVE-2025-21298	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows OLE cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022, 2025.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21298
3	CVE-2025-21297 CVE-2025-21309	- Điểm CVSS: 8.1 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Remote Desktop Services cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server 2012, 2016, 2019, 2022, 2025.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21297 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21309
4	CVE-2025-21308	- Điểm CVSS: 6.5 (Cao) - Mô tả: Lỗ hổng trong Windows Themes cho phép đối tượng tấn công thực hiện tấn công giả mạo	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21308

		(spoofing). Thông tin chi tiết về lỗ hổng đã được công bố công khai. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2012, 2016, 2019, 2022, 2025.	
5	CVE-2025-21186 CVE-2025-21366 CVE-2025-21395	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Access cho phép đối tượng tấn công thực thi mã từ xa. Thông tin chi tiết về lỗ hổng đã được công bố công khai. - Ảnh hưởng: Microsoft Access 2016, Microsoft Office LTSC 2021, 2024, Microsoft 365 Apps for Enterprise, Microsoft Office 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21186 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21366 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21395
6	CVE-2025-21275	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Windows App Package Installer cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Thông tin chi tiết về lỗ hổng đã được công bố công khai. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2022, 2025.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21275
7	CVE-2025-21311	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows NTLM V1 cho phép đối tượng tấn công thực hiện leo thang đặc quyền.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21311

		- Ảnh hưởng: Windows 11, Windows Server 2022, 2025.	
8	CVE-2025-21354 CVE-2025-21362	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office LTSC 2021, 2024, Microsoft 365 Apps for Enterprise, Microsoft Office 2019, Office Online Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21354 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21362
9	CVE-2025-21402	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office OneNote cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office LTSC 2021, 2024, Microsoft OneNote.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21402
10	CVE-2025-21365	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office LTSC 2024, Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21365
11	CVE-2025-21345 CVE-2025-21356	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office Visio cho	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21345

		phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office LTSC 2021, 2024, Microsoft 365 Apps for Enterprise, Microsoft Office 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21356
12	CVE-2025-21363	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office LTSC 2021, 2024, Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21363
13	CVE-2025-21357 CVE-2025-21361	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office LTSC 2021, 2024, Microsoft 365 Apps for Enterprise, Microsoft Office 2019, Microsoft Outlook 2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21357 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21361
14	CVE-2025-21344 CVE-2025-21348	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21344 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21348

3. Khuyến nghị giải pháp

Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng

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.

Kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng an toàn thông tin 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 tham khảo **mục 4** của báo cáo.*

4. Tài liệu tham khảo

https://msrc.microsoft.com/update-guide/

https://www.zerodayinitiative.com/blog/2025/1/14/the-january-2025-security-update-review