

# Báo cáo về các lỗ hổng an toàn thông tin trong các sản phẩm của Microsoft tháng 02/2025

## 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 11/02/2025, Microsoft đã phát hành danh sách bản vá **tháng 02** với tổng **67 lỗ hổng an toàn thông tin** gồm có **57 lỗ hổng an toàn thông tin** trong các sản phẩm của hãng Microsoft và **10 lỗ hổng an toàn thông tin** trong các sản phẩm thuộc bên thứ ba có ảnh hưởng tới Microsoft, trong đó có 03 lỗ hổng mức Nghiêm trọng, 53 lỗ hổng mức độ Cao và 01 lỗ hổng mức Trung bình.

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 Microsoft như: Windows và các thành phần của Windows, Office và các thành phần của Office, SharePoint Server,...

*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 **quynhlt@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](mailto: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 02/2025

STT	CVE	Mô tả	Link tham khảo
1	CVE-2025-21376	<ul style="list-style-type: none"> <li>- Điểm CVSS: 8.1 (Nghiêm trọng)</li> <li>- Mô tả: Lỗ hổng trong Windows Lightweight Directory Access Protocol (LDAP) cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Windows 10, 11, Windows Server 2012, 2016, 2019, 2022, 2025.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21376">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21376</a>
2	CVE-2025-21400	<ul style="list-style-type: none"> <li>- Điểm CVSS: 8.0 (Cao)</li> <li>- Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21400">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21400</a>
3	CVE-2025-21392 CVE-2025-21397	<ul style="list-style-type: none"> <li>- Điểm CVSS: 7.8 (Cao)</li> <li>- Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Microsoft Office 2016, Microsoft Office LTSC 2021, 2024, Microsoft 365 Apps for Enterprise, Microsoft Office 2019.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21392">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21392</a> <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21397">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21397</a>
4	CVE-2025-21381 CVE-2025-21386 CVE-2025-21387 CVE-2025-21390	<ul style="list-style-type: none"> <li>- Điểm CVSS: 7.8 (Nghiêm trọng)</li> <li>- Mô tả: Lỗ hổng trong Microsoft Excel cho phép</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21381">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21381</a>

	CVE-2025-21394	<p>đối tượng tấn công thực thi mã từ xa.</p> <p>- Ảnh hưởng: Microsoft Excel 2016, Microsoft Office LTSC 2021, 2024, Microsoft 365 Apps for Enterprise, Microsoft Office 2019.</p>	<p><a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21386">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21386</a></p> <p><a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21387">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21387</a></p> <p><a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21390">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21390</a></p> <p><a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21394">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21394</a></p>
5	CVE-2025-21418	<p>- Điểm CVSS: 7.8 (Cao)</p> <p>- Mô tả: Lỗ hổng trong Windows Ancillary Function Driver for WinSock cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.</p> <p>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022, 2025.</p>	<p><a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21418">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21418</a></p>
6	CVE-2025-21391	<p>- Điểm CVSS: 7.1 (Cao)</p> <p>- Mô tả: Lỗ hổng trong Windows Storage cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.</p> <p>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2016, 2019, 2022, 2025.</p>	<p><a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21391">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21391</a></p>

7	CVE-2025-21379	<ul style="list-style-type: none"> <li>- Điểm CVSS: 7.1 (Nghiêm trọng)</li> <li>- Mô tả: Lỗ hổng trong DHCP Client Service cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Windows Windows 11, Windows Server 2025.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21379">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21379</a>
8	CVE-2025-21377	<ul style="list-style-type: none"> <li>- Điểm CVSS: 6.5 (Cao)</li> <li>- Mô tả: Lỗ hổng trong Windows gây lộ lọt mã băm NTLM, cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). Thông tin chi tiết về lỗ hổng đã được công bố công khai.</li> <li>- Ảnh hưởng: Windows 10, 11, Windows Server 2012, 2016, 2019, 2022, 2025.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21377">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21377</a>

### 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/2025/2/11/the-february-2025-security-update-review>