

Số: /CATT-NCSC  
V/v lỗ hổng an toàn thông tin ảnh hưởng  
cao và nghiêm trọng trong các sản phẩm  
Microsoft công bố tháng 11/2023

Hà Nội, ngày tháng năm 2023

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 14/11/2023, Microsoft đã phát hành danh sách bản vá tháng 11 với 63 lỗ hổng an toàn thông tin trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý vào các lỗ hổng an toàn thông tin có mức ảnh hưởng cao và nghiêm trọng sau:

- Lỗ hổng an toàn thông tin **CVE-2023-36397** trong Windows Pragmatic General Multicast cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2023-36400** trong Windows HMAC Key Derivation cho phép đối tượng tấn công thực hiện leo thang đặc quyền.

- Lỗ hổng an toàn thông tin **CVE-2023-36025** cho phép đối tượng tấn công vượt qua tính năng bảo mật SmartScreen của Windows. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2023-36038** trong ASP.NET Core cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ (DoS). Thông tin chi tiết về lỗ hổng đã được công bố trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2023-36439** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2023-36033** trong Windows Desktop Manager cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2023-36036** trong Windows Cloud Files Mini Filter Driver cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2023-36041** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2023-36413** cho phép đối tượng tấn công vượt qua tính năng bảo mật của Microsoft Office. Thông tin chi tiết về lỗ hổng đã được công bố trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2023-38177** trong Microsoft SharePoint Server 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 tính 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: [ncsc@ais.gov.vn](mailto:ncsc@ais.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;
- Đơn vị chuyên trách về ATTT của: Văn phòng Trung ương Đảng; Văn phòng Quốc hội; Văn phòng Chủ tịch nước; Tòa án Nhân dân tối cao; Viện Kiểm sát Nhân dân tối cao;
- Các Cục: Viễn thông, Bưu điện Trung ương;
- Các Trung tâm: TTTT, VNNIC;
- Cục trưởng (để b/c);
- Các Phó Cục trưởng;
- P. ATHTTT, VNCERT/CC;
- Lưu: VT, NCSC.LTQ.

**KT. CỤC TRƯỞNG  
PHÓ CỤC TRƯỞNG**

**Trần Đăng Khoa**

**Phụ lục**  
**THÔNG TIN VỀ CÁC LỖ HỔNG AN TOÀN THÔNG TIN**  
**TRONG SẢN PHẨM MICROSOFT**

(Kèm theo Công văn số /CATTT-NCSC  
ngày / /2023 của Cục An toàn thông tin)

**1. Thông tin các lỗ hổng an toàn thông tin**

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-36397	<ul style="list-style-type: none"> <li>- Điểm: CVSS: 9.8 (Nghiêm trọng)</li> <li>- Mô tả: Lỗ hổng trong Windows Pragmatic General Multicast cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa.</li> <li>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36397">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36397</a>
2	CVE-2023-36400	<ul style="list-style-type: none"> <li>- Điểm: CVSS: 8.8 (Nghiêm trọng)</li> <li>- Mô tả: Lỗ hổng trong Windows HMAC Key Derivation cho phép đối tượng tấn công thực hiện leo thang đặc quyền.</li> <li>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2016, 2019, 2022.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36400">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36400</a>
3	CVE-2023-36025	<ul style="list-style-type: none"> <li>- Điểm: CVSS: 8.8 (Cao)</li> <li>- Mô tả: Lỗ hổng cho phép đối tượng tấn công vượt qua tính năng bảo mật SmartScreen của Windows. Lỗ hổng hiện đang bị khai thác trong thực tế.</li> <li>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36025">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36025</a>

STT	CVE	Mô tả	Link tham khảo
4	CVE-2023-36038	<ul style="list-style-type: none"> <li>- Điểm: CVSS: 8.2 (Cao)</li> <li>- Mô tả: Lỗ hổng trong ASP.NET Core cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ (DoS). Thông tin chi tiết về lỗ hổng đã được công bố trong thực tế.</li> <li>- Ảnh hưởng: ASP.NET Core, .NET, Visual Studio 2022.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36038">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36038</a>
5	CVE-2023-36439	<ul style="list-style-type: none"> <li>- Điểm: CVSS: 8.0 (Cao)</li> <li>- Mô tả: Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Microsoft Exchange Server 2016, 2019.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36439">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36439</a>
6	CVE-2023-36033	<ul style="list-style-type: none"> <li>- Điểm: CVSS: 7.8 (Cao)</li> <li>- Mô tả: Lỗ hổng trong Windows Desktop Manager cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.</li> <li>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2019, 2022.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36033">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36033</a>
7	CVE-2023-36036	<ul style="list-style-type: none"> <li>- Điểm: CVSS: 7.8 (Cao)</li> <li>- Mô tả: Lỗ hổng trong Windows Cloud Files Mini Filter Driver cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.</li> <li>- Ảnh hưởng: Windows 10, Windows 11,</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36036">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36036</a>

STT	CVE	Mô tả	Link tham khảo
		Windows Server 2019, 2022.	
8	CVE-2023-36041	- 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 Excel, Microsoft Office, Microsoft 365 Apps.	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36041">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36041</a>
9	CVE-2023-36413	- Điểm: CVSS: 6.5 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công vượt qua tính năng bảo mật của Microsoft Office. Thông tin chi tiết về lỗ hổng đã được công bố trong thực tế. - Ảnh hưởng: Microsoft Office, Microsoft 365 Apps.	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36413">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36413</a>
10	CVE-2023-38177	- Điểm: CVSS: 6.1 (Cao) - Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server 2016, 2019.	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38177">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38177</a>

## 2. Hướng dẫn khắc phục

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 nguồn tham khảo tại mục 1 của Phụ lục.

## 3. Tài liệu tham khảo

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

<https://www.zerodayinitiative.com/blog/2023/11/14/the-november-2023-security-update-review>