

Số: **H64** /TB-SGDĐT

Quảng Ngãi, ngày **21** tháng 4 năm 2022

## THÔNG BÁO

### **Cảnh báo lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm Microsoft công bố tháng 4/2022**

Theo đề nghị của Sở Thông tin và Truyền thông tại Công văn số 488/STTTT-BCVT&CNTT ngày 20/4/2022 về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm Microsoft công bố tháng 4/2022;

Sở Giáo dục và Đào tạo thông báo đến các đơn vị, cơ sở giáo dục có sử dụng sản phẩm Microsoft để nắm tình hình và triển khai cập nhật bản vá lỗi kịp thời để tránh nguy cơ bị tấn công đối với các thiết bị ảnh hưởng theo hướng dẫn của Microsoft (*tham khảo thông tin lỗ hổng và cách khắc phục tại Phụ lục đính kèm Công văn số 488/STTTT-BCVT&CNTT ngày 20/4/2022 của Sở Thông tin và Truyền thông*);

Khi phát hiện các hệ thống có biểu hiện bị khai thác, tấn công mạng, triển khai ngay các biện pháp xử lý ngăn chặn tấn công trên hệ thống và thông tin về Văn phòng Sở Giáo dục và Đào tạo qua điện thoại: 0255.3824164 – 0914121856, Email: [ndhuan-sgd@quangngai.gov.vn](mailto:ndhuan-sgd@quangngai.gov.vn) ; [ndhuan@quangngai.edu.vn](mailto:ndhuan@quangngai.edu.vn) để phối hợp xử lý.

Yêu cầu lãnh đạo các đơn vị quan tâm chỉ đạo thực hiện./.

**Nơi nhận:**

- Đơn vị trực thuộc Sở GDĐT;
- Phòng GDĐT huyện, thị xã, thành phố;
- Trung tâm GDNN-GDTX huyện, thị xã;
- Lãnh đạo Sở GDĐT;
- Các phòng thuộc Sở GDĐT;
- Lưu: VT, VP, ndh.

**TL. GIÁM ĐỐC**  
**KT. CHÁNH VĂN PHÒNG**  
**PHÓ CHÁNH VĂN PHÒNG**



**Nguyễn Đức Huân**

## PHỤ LỤC

**THÔNG TIN VỀ CÁC LỖ HỒNG BẢO MẬT TRONG MICROSOFT**  
(Kèm theo Công văn số **488** STTTT-BCVT&CNTT ngày **20/4/2022** của Sở Thông tin và Truyền thông)

## 1. Thông tin các lỗ hồng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-26809	<ul style="list-style-type: none"> <li>- Điểm CVSS: 9.8 (Nghiêm trọng)</li> <li>- Lỗ hồng trong RPC Runtime Library cho phép đối tượng tấn công thực thi mã từ xa với đặc quyền cao trên hệ thống bị ảnh hưởng.</li> <li>- Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022.</li> </ul>	<a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-26809">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-26809</a>
2	CVE-2022-24491	<ul style="list-style-type: none"> <li>- Điểm CVSS: 9.8 (Nghiêm trọng)</li> <li>- Lỗ hồng trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa với đặc quyền cao.</li> <li>- Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012 /2016/2019.</li> </ul>	<a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-24491">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-24491</a>
3	CVE-2022-24497	<ul style="list-style-type: none"> <li>- Điểm CVSS: 9.8 (Nghiêm trọng)</li> <li>- Lỗ hồng trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Windows 8.1/10, Windows Server 2012/2016/2019/2022.</li> </ul>	<a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-24497">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-24497</a>
4	CVE-2022-26815	<ul style="list-style-type: none"> <li>- Điểm CVSS: 7.2 (cao)</li> <li>- Lỗ hồng trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022.</li> </ul>	<a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-26815">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-26815</a>
5	CVE-2022-	- Điểm CVSS: 7.9 (cao)	<a href="https://msrc.microsoft.com">https://msrc.microsoft.com</a>

STT	CVE	Mô tả	Link tham khảo
	26904	- Lỗ hổng trong Windows User Profile Service cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã có mã khai thác công khai trên Internet. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016.	<a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-26904">m/updateguide/vulnerability/CVE-2022-26904</a>
6	CVE-2022-26919	- Điểm CVSS: 8.1 (Cao) - Lỗ hổng trong Windows LDAP cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	<a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-26919">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-26919</a>
7	CVE-2022-24521	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Windows Common Log File System Driver cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	<a href="https://msrc.microsoft.com/updateguide/enUS/vulnerability/CVE-2022-24521">https://msrc.microsoft.com/updateguide/enUS/vulnerability/CVE-2022-24521</a>

## 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-Apr>

<https://www.zerodayinitiative.com/blog/2022/4/11/the-april-2022-security-pdate-review>