ỦY BAN NHÂN DÂN
HUYỆN NHÀ BÈ
PHÒNG GIÁO DỤC VÀ ĐÀO TẠO

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

PHỤ LỤC 2
Thông tin về các lỗ hổng tồn tại trên các sản phẩm phổ biến

*(Kèm theo Công văn số*112 */GDĐT ngày 16 tháng 01 năm 2025*
của Phòng Giáo dục và Đào tạo huyện Nhà Bè)

1. Thông tin các lỗ hổng an toàn thông tin

TT	Mã điểm yếu/lỗ hổng	Mô tả	Ghi chú
1	CVE-2024-23897	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: Jenkins - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-23897
2	CVE-2023-45249	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Ảnh hưởng: Acronis Cyber Infrastructure - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2023-45249
3	CVE-2024-39717	- Điểm CVSS: 7.2 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Ảnh hưởng: Versa Director GUI - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-39717
4	CVE-2024-6800	- Điểm CVSS: N/A - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Ảnh hưởng: GitHub Enterprise Server - Lỗ hổng chưa có mã khai thác và chưa bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-6800
5	CVE-2024-7589	- Điểm CVSS: 8.1 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: FreeBSD - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-7589

TT	Mã điểm yếu/lỗ hổng	Mô tả	Ghi chú
6	CVE-2024-7593	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép - Ảnh hưởng: Ivanti vTM - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-7593
7	CVE-2024-28000	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền. - Ảnh hưởng: LiteSpeed Technologies LiteSpeed Cache - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-28000
8	CVE-2024-37085	- Điểm CVSS: 7.2 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: VMware ESXi - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-37085
9	CVE-2024-38077	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows Server 2022, Windows Server 2016. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-38077
10	CVE-2024-38063	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Windows 10 - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-38063
11	CVE-2024-6387	- Điểm CVSS: 8.1 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: OpenSSH. - Lỗ hổng đã có mã khai thác và đang bị khai	https://nvd.nist.gov/vuln/detail/CVE-2024-6387

TT	Mã điểm yếu/lỗ hổng	Mô tả	Ghi chú
		thác trong thực tế.	
12	CVE-2024-40766	- Điểm CVSS: N/A - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: SonicWall SonicOS - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-40766

2. Danh sách top 10 điểm yếu, lỗ hổng tồn tại phổ biến

TT	Mã điểm yếu/ lỗ hổng	SL máy bị ảnh hưởng	Ghi chú
1	CVE-2022-26809	15468	https://nvd.nist.gov/vuln/detail/ CVE-2022-26809
2	CVE-2023-21716	6697	https://nvd.nist.gov/vuln/detail/ CVE-2023-21716
3	CVE-2024-8035	5324	https://nvd.nist.gov/vuln/detail/ CVE-2023-8035
4	CVE-2024-8198	2334	https://nvd.nist.gov/vuln/detail/ CVE-2021-8198
5	CVE-2024-38223	2050	https://nvd.nist.gov/vuln/detail/ CVE-2024-38223
6	CVE-2024-7256	1844	https://nvd.nist.gov/vuln/detail/ CVE-2024-7256
7	CVE-2024-7550	1631	https://nvd.nist.gov/vuln/detail/ CVE-2021-7550
8	CVE-2024-7531	1595	https://nvd.nist.gov/vuln/detail/ CVE-2023-7531
9	CVE-2021-40444	992	https://nvd.nist.gov/vuln/detail/ CVE-2024-40444
10	CVE-2021-28310	781	https://nvd.nist.gov/vuln/detail/ CVE-2020-28310

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 ghi chú.

3. Tài liệu kham khảo

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

https://www.zerodayinitiative.com/blog/2024/8/13/the-august-2024-security-update-review