UBND HUYỆN ĐỊNH HÓA
PHÒNG VĂN HÓA VÀ TT

Số:84 /VHTT-TT

V/v lỗ hổng bảo mật ảnh hưởng nghiêm trọng trong phần mềm PAN-OS và lỗ hổng an toàn thông tin trong các sản phẩm của hãng Microsoft công bố tháng 4/2024

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

Định Hóa, ngày 23 tháng 4 năm 2024

Kính gửi:
- Các cơ quan, ban, ngành, đoàn thể huyện;
- Ủy ban nhân dân các xã, thị trấn;
- Các doanh nghiệp viễn thông trên địa bàn huyện.

Thực hiện Công văn số 835/STTTT-CNTT ngày 17/4/2024 của Sở Thông tin và Truyền thông về lỗ hổng bảo mật ảnh hưởng nghiêm trọng trong phần mềm PAN-OS và lỗ hổng an toàn thông tin trong các sản phẩm của hãng Microsoft công bố tháng 4/2024.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan, đơn vị, góp phần đảm bảo an toàn cho các hệ thống thông tin dùng chung, liên thông của tỉnh; Phòng Văn hóa và Thông tin thông tin đến các cơ quan, đơn vị, doanh nghiệp viễn thông, UBND các xã, thị trấn về lỗ hổng bảo mật ảnh hưởng nghiêm trọng trong phần mềm PAN-OS khuyến nghị về các lỗ hổng bảo mật có mức ảnh hưởng nghiêm trọng, mức ảnh hưởng cao trong các sản phẩm của hãng Microsoft công bố tháng 4/2024 và hướng dẫn khắc phục.

(Chi tiết thông tin về các lỗ hổng bảo mật và hướng dẫn khắc phục tại phụ lục đính kèm)

Căn cứ các nội dung nêu trên, Phòng Văn hóa và Thông tin đề nghị UBND các xã, thị trấn, các cơ quan, đơn vị, doanh nghiệp viễn thông quan tâm triển khai thực hiện; trong quá trình thực hiện nếu có khó khăn, vướng mắc, phản ánh kịp thời về Phòng Văn hóa và Thông tin để được hướng dẫn, hỗ trợ. Thông tin đầu mối liên hệ: Ông Ngô Nguyên Long, công chức biệt phái Phòng Văn hóa và Thông tin, số điện thoại 0943905333./.

Nơi nhận:
- Như trên;
- Lãnh đạo UBND huyện;
- Lưu: VT, VHTT.

KT. TRƯỞNG PHÒNG
PHÓ TRƯỞNG PHÒNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
PHÒNG VĂN HÓA VÀ THÔNG TIN
H. ĐỊNH HÓA - T. THÁI NGUYÊN

Ngô Hoàng

PHỤ LỤC I: THÔNG TIN VỀ LỖ HỔNG BẢO MẬT ẢNH HƯỞNG NGHIÊM TRỌNG TRONG PHẦN MỀM PAN-OS

*(Kèm theo Công văn số:*84 */ VHTT-TT ngày 23 / 4/2024*
của Phòng Văn hóa và Thông tin)

I. THÔNG TIN LỖ HỔNG ẢNH HƯỞNG NGHIÊM TRỌNG TRONG PHẦN MỀM PAN-OS

1. Thông tin lỗ hổng bảo mật

Mô tả: Lỗ hổng CVE-2024-3400 (Điểm CVSS: 10) ảnh hưởng trên phần mềm PAN-OS trong gateway GlobalProtect hiện đang bị sử dụng để khai thác. Đối tượng tấn công khai thác lỗ hổng chèn lệnh này có thể thực thi mã từ xa với quyền root trên tường lửa. Lỗ hổng gây ảnh hưởng cho tường lửa cấu hình trên GlobalProtect gateway và telemetry của thiết bị.

Lỗ hổng này ảnh hưởng đến các phiên bản:

- PAN-OS 11.1 trước bản 11.1.2-h3
- PAN-OS 11.0 trước bản 11.0.4-g1
- PAN-OS 10.2 trước bản 10.2.9-h1

- Bản vá cho các phiên bản bị ảnh hưởng sẽ được phát hành ngày 14/04/2024, người dùng nên cập nhật ngay khi khả dụng.

Dưới đây là một số IoC được ghi nhận:

- Update.py
- 3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac
- 5460b51da26c060727d128f3b3d6415d1a4c25af6a29fef4cc6b867ad3659078
- 172.233.228[.]93
- hxxp://172.233.228[.]93/policy
- hxxp://172.233.228[.]93/patch
- 66.235.168[.]222

2. Hướng dẫn khắc phục

Trước mắt, người dùng nên bật Threat ID 95187 và đảm bảo các biện pháp bảo mật lỗ hổng đã được áp dụng cho GlobalProtect. Trong trường hợp không thể bật Threat ID 95187, người dùng nên tạm thời tắt chức năng telemetry trên thiết bị cho tới cập nhật bản vá và chỉ nên bật lại sau khi đã cập nhật bản vá. Các bước để thực hiện việc tắt telemetry như sau:

1. Device > Setup >Telemetry;
2. Chọn widget Telemetry;

3. Bỏ chọn mục “Enable Telemetry”;
4. Bấm OK để lưu thay đổi.

3. Tài liệu tham khảo

https://security.paloaltonetworks.com/CVE-2024-3400

https://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-040

II. THÔNG TIN CÁC LỖ HỔNG BẢO MẬT TRONG CÁC SẢN PHẨM CỦA HÃNG MICROSOFT CÔNG BỐ THÁNG 4/2024

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-20678	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Remote Procedure Call Runtime (RPC) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20678
2	CVE-2024-29988	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong SmartScreen cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29988
3	CVE-2024-21322 CVE-2024-21323 CVE-2024-29053	- Điểm: CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft Defender for IoT cho phép đối tượng tấn công thực thi mã từ	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21322 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21323 https://msrc.microsoft.com/updat

		xa. - Ảnh hưởng: Microsoft Defender for IoT.	e-guide/vulnerability/CVE-2024-29053
4	CVE-2024-20670	- Điểm: CVSS: 8.1 (Cao) - Mô tả: Lỗ hổng trong Outlook for Windows làm lộ lọt NTML hash, cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). - Ảnh hưởng: Outlook for Windows.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20670
5	CVE-2024-26256	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong thư viện nguồn mở libarchive cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 11; Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26256
6	CVE-2024-26257	- 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 365 Apps for Enterprise, Microsoft Office LTSC for Mac.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26257

7	CVE-2024-26221 CVE-2024-26222 CVE-2024-26223 CVE-2024-26224 CVE-2024-26227 CVE-2024-26231 CVE-2024-26233	- Điểm: CVSS: 7.2 (Cao) - Mô tả: Lỗ hổng trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26221 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26222 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26223 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26224 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26227 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26231 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26233
8	CVE-2024-26234	- Điểm: CVSS: 6.7 (Cao) - Mô tả: Lỗ hổng trong Proxy Driver cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26234

2. Hướng dẫn khắc phục

- Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin, đề nghị các cơ quan, đơn vị, địa phương chỉ đạo bộ phận chuyên trách về công nghệ thông tin/an toàn thông tin phối hợp với bộ phận có liên quan thực hiện kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng và tiến hành cập nhật bản vá kịp thời cho các lỗ hổng bảo mật nói trên theo hướng dẫn của hãng để tránh nguy cơ bị tấn công.

- 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.

- Tuyên truyền thường xuyên, liên tục tới toàn thể cán bộ, công chức, viên chức, người lao động của cơ quan, đơn vị mình nhằm nâng cao nhận thức và trang bị kỹ năng đảm bảo an toàn thông tin trên không gian mạng.

- Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ:

+ Ông Ngô Nguyên Long, công chức biệt phái Phòng Văn hóa và Thông tin, số điện thoại: 0943.905.333.

4. Tài liệu tham khảo

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

https://www.zerodayinitiative.com/blog/2024/4/9/the-april-2024-security-updates-review