UBND TỈNH TÂY NINH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 1760 /STTTT-TTGSĐH
V/v cảnh báo lỗ hổng bảo mật có mức ảnh hưởng Cao trong các sản phẩm Microsoft công bố tháng 11 và FortiOS, FortiProxy

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

Tây Ninh, ngày15 tháng 11 năm 2022

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các cơ quan tham mưu, giúp việc Tỉnh ủy;
- Mặt trận Tổ quốc và các Đoàn thể chính trị - xã hội;
- Các Sở, ban, ngành tỉnh;
- Các huyện, thị, thành ủy trực thuộc Tỉnh ủy;
- UBND các huyện, thị xã, thành phố.

Thực hiện theo Công văn số 1824/CATTT-NCSC và Công văn số 1547/CATTT-NCSC của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 11/2022 và cảnh báo lỗ hổng bảo mật ảnh hưởng nghiêm trọng trong FortiOS và FortiProxy *(Thông tin chi tiết phụ lục kèm theo)*.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin cho người dùng, đơn vị và toàn bộ hệ thống của tỉnh, Sở Thông tin và Truyền thông đề nghị các đơn vị, địa phương thực hiện gấp các công việc cụ thể như sau:

1. Kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows và phần mềm 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 gửi kèm theo).

2. Kiểm tra, rà soát các sản phẩm FortiOS và FortiProxy đang sử dụng có khả năng bị ảnh hưởng bởi lỗ hổng trên. Thực hiện nâng cấp lên phiên bản mới nhất để tránh nguy cơ bị tấn công; trong trường hợp chưa thể nâng cấp cần thực hiện thiết lập chính sách để hạn chế quyền truy cập các địa chỉ IP vào giao diện quản trị (tham khảo thông tin tại Phụ lục gửi kèm theo).

3. Tăng cường kiểm tra, giám sát hệ thống mạng của đơn vị, địa phương, khi có phát hiện hoạt động tấn công mạng, đề nghị liên hệ Sở Thông tin và Truyền thông để phối hợp xử lý kịp thời.

Thông tin liên quan đề nghị liên hệ Ông Vương Duy Thanh - Trung tâm Giám sát, điều hành kinh tế, xã hội tập trung; Điện thoại: 0932624462.

Trân trọng./.

Nơi nhận:
- Như trên;
- GĐ Sở (b/c);
- P. CNTTBCVT;
- Lưu: VT, TTGSĐH.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH TÂY NINH

Nguyễn Trung Hiếu

PHỤ LỤC
Thông tin các lỗ hổng nghiêm trọng trong các sản phẩm Microsoft công bố tháng 11 và FortiOS, FortiProxy

1.Thông tin lỗ hổng bảo mật

1.1. Thông tin lỗ hổng bảo mật Microsoft công bố tháng 11

- Mô tả:

+ 06 lỗ hổng bảo mật **CVE-2022-41082, CVE-2022-41040, CVE-2022-41080, CVE-2022-41079, CVE-2022-41078, CVE-2022-41123** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa, nâng cao đặc quyền. Trong đó, 02 lỗ hổng CVE-2022-41082, CVE-2022-41040 đã được cảnh báo tại văn bản số 1484/CATTT-VNCERT/CC về việc cảnh báo lỗ hổng bảo mật zero-day ảnh hưởng nghiêm trọng đến Microsoft Exchange phát hành ngày 30/9/2022.

+ 02 lỗ hổng bảo mật **CVE-2022-41128, CVE-2022-41118** trong Windows Scripting Languages cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đang bị khai thác trong thực tế.

+ Lỗ hổng bảo mật **CVE-2022-41091** trong Windows Mark of the Web cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật.

+ Lỗ hổng bảo mật **CVE-2022-41073** trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

+ Lỗ hổng bảo mật **CVE-2022-41125** trong Windows CNG Key Insolation Service cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

+ 03 lỗ hổng bảo mật **CVE-2022-41044, CVE-2022-41088, CVE-2022-41039** trong Windows Point-to-Point cho phép đối tượng tấn công thực thi mã từ xa.

+ 04 lỗ hổng bảo mật **CVE-2022-41105, CVE-2022-41106, CVE-2022-41063, CVE-2022-41104** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa, tấn công giả mạo (Spoofing), thực hiện tấn công vượt qua cơ chế bảo mật.

- Ảnh hưởng:

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-41082, CVE-2022-41040, CVE-2022-41080, CVE-2022-41079, CVE-2022-41078,	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa, nâng cao đặc quyền.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41082 https://msrc.microsoft.com/update-

	CVE-2022-41123	- Ảnh hưởng: Microsoft Exchange Server 2016 CU 23/22, Exchange Server 2019 CU 11, Exchange Server 2013 CU 23	guide/vulnerability/CVE-2022-41040 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41080 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41123 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41078 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41079
2	CVE-2022-41128, CVE-2022-41118	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong trong Windows Scripting Languages cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41128 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41118
3	CVE-2022-41091	- Điểm CVSS: 5.4 (Trung bình) - Lỗ hổng trong Windows Mark of the Web cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật. - Ảnh hưởng: Windows 10/11, Windows Server 2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41091

4	CVE-2022-41073	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41073
5	CVE-2022-41125	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng Windows CNG Key Insolation Service cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019/2022	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41125
6	CVE-2022-41044, CVE-2022-41088, CVE-2022-41039	- Điểm CVSS: 8.1 (Cao) - Lỗ hổng trong Windows Point-to-Point cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41044 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41088 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41039
7	CVE-2022-41105, CVE-2022-41106, CVE-2022-41063, CVE-2022-41104	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa, tấn công giả mạo (Spoofing), thực hiện tấn công vượt qua cơ chế bảo mật.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41105 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41106

		- Ảnh hưởng: Microsoft Excel 2013/2016, Microsoft Office, Microsoft 365.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41063 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41104

- Đánh giá mức độ: Đánh giá sơ bộ từ các chuyên gia bảo mật, lỗ hổng này ảnh hưởng đến nhiều thiết bị trên toàn cầu trong đó có cả Việt Nam. Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) đánh giá khả năng các mã khai thác của các lỗ hổng này sẽ sớm được công khai trên Internet trong thời gian sắp tới.

1.2. Thông tin lỗ hổng bảo mật trong FortiOS và FortiProxy

- Mô tả: Lỗ hổng ảnh hưởng đến FortiOS và FortiProxy, cho phép đối tượng tấn công chưa xác thực có quyền truy cập vào giao diện quản trị từ xa thông qua HTTP/HTTPS requests độc hại.

- Ảnh hưởng: FortiOS phiên bản 7.0.0 đến 7.0.6; 7.2.0 đến 7.2.1, FortiProxy phiên bản 7.0.0 đến 7.0.6, 7.2.0.

2. Hướng dẫn khắc phục:

2.1. Lỗ hổng bảo mật Microsoft công bố tháng 11

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.

2.2. Lỗ hổng bảo mật trong FortiOS và FortiProxy

Biện pháp tốt nhất để khắc phục lỗ hổng bảo mật nói trên là cập nhật lên phiên bản mới (FortiOS 7.0.7 và 7.2.2, FortiProxy 7.0.7 và 7.2.1). Trong trường hợp chưa thể nâng cấp, Quý đơn vị cần thực hiện biện pháp khắc phục tạm thời bằng cách thiết lập chính sách và hạn chế quyền truy cập các địa chỉ IP vào giao diện quản trị, triển khai xác thực đa yếu tố (MFA) để không bị lộ thông tin giao diện quản trị và tránh nguy cơ bị tấn công khai thác.

3. Nguồn tham khảo:

3.1. Lỗ hổng bảo mật Microsoft công bố tháng 11

https://msrc.microsoft.com/update-guide/releaseNote/2022-Nov

https://www.zerodayinitiative.com/blog/2022/11/8/the-november-2022-security-update-review

3.2. Lỗ hổng bảo mật trong FortiOS và FortiProxy

https://www.tenable.com/blog/cve-2022-40684-critical-authentication-bypass-in-fortios-and-fortiproxy

https://docs.fortinet.com/document/fortigate/7.2.2/fortios-release-notes/289806/resolved-issues

https://docs.fortinet.com/document/fortigate/7.2.0/best-practices/127480/user-authentication-for-management-network-access