BỘ THÔNG TIN TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

Số: 1410/CATTT-NCSC
V/v lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft

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

Hà Nội, ngày 14 tháng 10 năm 2021

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.

Vừa qua, Microsoft đã phát hành danh sách bản vá tháng 10 với 78 lỗ hổng bảo mật trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý các lỗ hổng bảo mật sau:

- Lỗ hổng bảo mật CVE-2021-26427 trong Microsoft Exchange Server: Lỗ hổng này được coi là ít có khả năng bị khai thác, nhưng vẫn có thể cho phép đối tượng tấn công thực thi mã từ xa trên máy chủ mục tiêu. Điều này cho thấy, Exchange Server vẫn là mục tiêu hàng đầu của các nhóm tấn công có chủ đích (APT) từ tháng 3/2021 đến nay và có nhiều cách khai thác mà kẻ tấn công có thể tận dụng. Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin cũng đã đặc biệt nhấn mạnh tầm ảnh hưởng của Exchange Server thông qua nhiều văn bản cảnh báo rộng rãi về các lỗ hổng bảo mật trong Exchange Server trước đây.

- Lỗ hổng bảo mật CVE-2021-40486 trong Microsoft Word: Lỗ hổng có điểm CVSS: 7.8 (cao) cho phép đối tượng tấn công thực thi mã từ xa mà không cần xác thực, từ đó có thể hoàn toàn chiếm quyền truy cập hệ thống mục tiêu.

- Lỗ hổng bảo mật CVE-2021-40469 trong Windows DNS Server: Lỗ hổng có điểm CVSS: 7.8 (cao), ảnh hưởng đến các phiên bản khác nhau của Windows 7/8.1/10. Để khai thác lỗ hổng này, đối tượng tấn công cần xác thực để thực thi mã

từ xa.

- 05 lỗ hổng bảo mật (CVE-2021-40471, CVE-2021-40473, CVE-2021-40474, CVE-2021-40479, CVE-2021-40485) trong Microsoft Excel: có điểm CVSS: 7.8 (cao), cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2021-40465 trong Windows Text Shaping: Lỗ hổng có điểm CVSS: 7.8 (cao) cho phép đối tượng tấn công thực thi mã từ xa mà không cần xác thực.

- Lỗ hổng bảo mật CVE-2021-41342 trong Windows MSHTML: Lỗ hổng có điểm CVSS: 6.8 (cao) cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2021-36970 trong Windows Print Spooler: Lỗ hổng có điểm CVSS: 8.8 (cao) cho phép đối tượng tấn công thực hiện tấn công giả mạo.

- 02 lỗ hổng bảo mật (CVE-2021-40461 và CVE-2021-38672) trong Windows Hyper-V: Các lỗ hổng này cho phép đối tượng tấn công thực thi mã từ xa, gây lỗi cấp phát bộ nhớ từ đó có thể đọc bộ nhớ trong của máy chủ.

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 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: ais@mic.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;
- Cục trưởng;
- Lưu: VT, NCSC.

CỤC TRƯỞNG

Nguyễn Thành Phúc

Phụ lục

Thông tin về các lỗ hổng bảo mật trong Pulse Connect Secure

(Kèm theo Công văn số /CATTT-NCSC ngày / /2021 của Cục An toàn thông tin)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2021-26427	- CVSS: 9.0 (cao) - Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26427
2	CVE-2021-41344 CVE-2021-40487	- CVSS: 8.1 (cao) - Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40487 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-41344
3	CVE-2021-40469	- CVSS: 7.2 (cao) - Lỗ hổng trong Windows DNS Server, cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40469
4	CVE-2021-40486	- CVSS: 7.8 (cao) - Lỗ hổng trong Microsoft Word, cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40486
5	CVE-2021-38672 CVE-2021-40461	- CVSS: 8.0 (cao) - Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38672https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40461

6	CVE-2021-40471 CVE-2021-40473 CVE-2021-40374 CVE-2021-40479 CVE-2021-40485	- CVSS: 7.8 (cao) - Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40471 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40473 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40474 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40479 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40485
7	CVE-2021-40480 CVE-2021-40481	- CVSS: 7.8 (cao) - Lỗ hổng trong Microsoft Office Visio cho phép đối tượng tấn công thực thi mã từ xa	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40480 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40481
8	CVE-2021-41330	- CVSS: 7.8 (cao) - Lỗ hổng trong Microsoft Windows Media Foundation cho phép đối tượng tấn công thực thi mã từ xa	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-41330
9	CVE-2021-41342	- CVSS: 6.8 (cao) - Lỗ hổng trong Windows MSHTML cho phép đối tượng tấn công thực thi mã từ xa	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-41342

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/en-us