BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

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

Số: 282 /TTCNTT-KTHT
V/v nguy cơ tấn công vào các cơ quan tổ chức qua lỗ hổng Zerologon

Hà Nội, ngày 18 tháng 9 năm 2020

Kính gửi: Các đơn vị trực thuộc Bộ (có hệ thống công nghệ thông tin)

Ngày 11/8/2020 Microsoft đã công bố lỗ hổng **CVE-2020-1472** (còn được gọi là **Zerologon)** trên các máy chủ Domain Controller cho phép đối tượng tấn công thực hiện tấn công leo thang để chiếm quyền quản trị. Domain Controller là máy chủ đóng vai trò trung tâm trong hệ thống mạng triển khai theo mô hình quản lý tập trung, dùng để xác thực và quản lý các máy trạm khác. Khi tấn công được vào máy chủ này, thì đối tượng tấn công xem như kiểm soát toàn bộ hệ thống thông tin của tổ chức.

Theo đánh giá sơ bộ, lỗ hổng này có thể ảnh hưởng đến nhiều cơ quan, tổ chức ở Việt Nam, đặc biệt là cơ quan chính phủ, ngân hàng, tổ chức tài chính, tập đoàn, doanh nghiệp và các công ty lớn, do các đơn vị này đều triển khai mô hình mạng có sử dụng máy chủ Domain Controller để thuận tiện cho việc quản lý.

Đầu tháng 9/2020, một số mã khai thác đã được công khai trên Internet và cảnh báo chính thức từ Trung tâm Giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin, Bộ Thông tin và Truyền thông. Những mã khai thác này có thể sử dụng để tấn công vào máy chủ Domain Controller qua đó kiểm soát hệ thống thông tin của các cơ quan tổ chức trong các chiến dịch tấn công nguy hiểm. Trong khi đó đến Quý I năm 2021, Microsoft dự kiến mới phát hành bản vá đầy đủ cho lỗ hổng trên.

Hiện tại, một số nhóm chuyên thực hiện tấn công APT có dấu hiệu tận dụng lỗ hổng này để tấn công sâu vào hệ thống thông tin của các cơ quan tổ chức. Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của quý đơn vị, Trung tâm Công nghệ thông tin yêu cầu đơn vị triển khai quyết liệt một số khuyến nghị sau:

1. Kiểm tra, rà soát và có phương án ngăn chặn các nhóm đối tượng tấn công tận dụng lỗ hổng để thực hiện các chiến dịch tấn công APT nguy hiểm.

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng. Đối với các cơ quan tổ chức có nhân sự kỹ thuật tốt có thể thử nghiệm xâm nhập vào hệ thống thông qua lỗ hổng này.

Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Trung tâm Công nghệ thông tin: Phòng Kỹ thuật hạ tầng, điện thoại 024.39439060, thư điện

tử: phongktht@most.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Bùi Thế Duy;
- Lưu: VT, KTHT.

GIÁM ĐỐC

Hà Quốc Trung

Phụ lục
Thông tin về lỗ hổng
(kèm theo Công văn số /TTCNTT-KTHT ngày / /2020)

1. Thông tin chung

- Điểm CVSS: 10.0 (đặc biệt nghiêm trọng)

- Ảnh hưởng: các máy chủ Domain Controller sử dụng Windows Server 2008; 2012; 2016; 2019, Windows Server Version 1903, 1909, 2004.

- Lỗ hổng tồn tại khi đối tượng tấn công thiết lập kết nối kênh bảo mật Netlogon với bộ điều khiển tên miền (Domain Controller), sử dụng giao thức từ xa Netlogon (MS-NRPC).

- Để khai thác lỗ hổng, đối tượng tấn công sẽ được yêu cầu sử dụng MSNRPC để kết nối với Domain Controller, để có quyền truy cập quản trị viên.

2. Hướng dẫn cập nhật bản vá

Microsoft đang giải quyết lỗ hổng này trong bản phát hành theo từng giai đoạn, quản trị viên tại cơ quan tổ chức trước mắt có thể cần thực hiện bản vá của Giai đoạn 1.

- Giai đoạn 1 (thực hiện ngay): cập nhật bản vá đã phát hành vào 11/8/2020. Bản vá này cho phép Domain Controller có thể bảo vệ các Windows, ghi lại các sự kiện để phát hiện thiết bị không tuân thủ đang sử dụng các kết nối kênh bảo mật Netlogon dễ bị tấn công.

Tham khảo các bản vá được cập nhật tại:

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

https://support.microsoft.com/en-us/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc

- Giai đoạn 2: bản vá phát hành Quý I năm 2021 sẽ khắc phục hoàn toàn.