UBND THÀNH PHỐ HẢI PHÒNG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 1913/STTTT-CNTT
V/v nguy cơ tấn công vào các cơ quan tổ chức qua lỗ hổng Zerologon.

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

Hải Phòng, ngày 18 tháng 9 năm 2020

Kính gửi:
- Các Sở, ban, ngành thành phố;
- Các cơ quan Trung ương tổ chức theo ngành dọc;
- Ủy ban nhân dân các quận, huyện;
- Các tổ chức, doanh nghiệp trên địa bàn.

Ngày 15/9/2020, Cục An toàn thông tin có Công văn số 797/CATTT-NCSC về việc nguy cơ tấn công vào các cơ quan tổ chức qua lỗ hổng CVE-2020-1472 (còn được gọi là Zerologon) trên các máy chủ Domain Controller, cảnh báo về lỗ hổng Zerologon và hướng dẫn cách xử lý, khắc phục lỗ hổng trên *(gửi kèm văn bản)*,

Sở Thông tin và Truyền thông trân trọng đề nghị các cơ quan, đơn vị rà soát hệ thống công nghệ thông tin và thực hiện các biện pháp phát hiện, ngăn chặn nguy cơ gây mất an toàn thông tin do lỗ hổng Zerologon gây ra tại các đơn vị và các cơ quan trực thuộc theo hướng dẫn của Cục An toàn thông tin tại Công văn số 797/CATTT-NCSC.

Sở Thông tin và Truyền thông cử ông Nguyễn Đông Huy (Trưởng Phòng Hạ tầng kỹ thuật và An toàn thông tin - Trung tâm Thông tin và Truyền thông, số điện thoại 098.4462472) là đầu mối phối hợp, trao đổi thông tin.

Trân trọng./.

Nơi nhận:
- Như trên;
- UBNDTP (để b/c);
- Ban 114 (để b/c);
- GĐ, các PGĐ Sở;
- TT.TTTT;
- Cổng TTĐT Sở, Cổng TTTP;
- Lưu: VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
THÀNH PHỐ HẢI PHÒNG

Lê Văn Kiên

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

Số: 797/CATTT-NCSC
V/v nguy cơ tấn công vào các cơ quan tổ chức qua lỗ hổng Zerologon

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

Hà Nội, ngày 15 tháng 9 năm 2020

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.

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, qua công tác theo dõi, giám sát an toàn thông tin, Trung tâm Giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin phát hiện có một số mã khai thác công khai trên Internet. 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 việc phát hành bản vá đầy đủ cho lỗ hổng Microsoft dự kiến đến Quý 1 năm 2021 mới hoàn thành.

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, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Cục An toàn 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.

3.Trong trường hợp hướng dẫn, kiểm tra chi tiết về lỗ hổng 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 (NCSC), điện thoại 02432091616, thư điện tử: ais@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Phạm Anh Tuấn (để b/c);
- Cục trưởng (để b/c);
- Phó Cục trưởng Nguyễn Khắc Lịch;
- Lưu: VT, NCSC.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Khắc Lịch

Phụ lục
Thông tin về lỗ hổng
(kèm theo Công văn số 7997/CATTT-NCSC ngày 15/9/2020)

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 MS-NRPC 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 1 năm 2021 sẽ khắc phục hoàn toàn