

Số: /STTTT-CNTT  
Về nguy cơ tấn công vào các cơ quan,  
tổ chức qua lỗ hổng Zerologon

Tuyên Quang, ngày tháng 9 năm 2020

Kính gửi:

- Văn phòng Hội đồng nhân dân tỉnh;
- Văn phòng Ủy ban nhân dân tỉnh;
- Các sở, ban, ngành;
- Ủy ban nhân dân các huyện, thành phố;
- Trung tâm Công nghệ thông tin và Truyền thông,  
Sở Thông tin và Truyền thông.

Căn cứ Văn bản số 797/CATTT-NCSC ngày 15/9/2020 của Cục An toàn thông tin về việc nguy cơ tấn công vào các cơ quan, tổ chức qua lỗ hổng Zerologon; Sở Thông tin và Truyền thông cung cấp thông tin và đưa ra các giải pháp phòng, tránh việc khai thác lỗ hổng Zerologon, cụ thể như sau:

### **1. Sơ lược về lỗ hổng Zerologon**

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 I năm 2021 mới hoàn thành.

## **2. Các giải pháp phòng, tránh**

Hiện tại, các cuộc 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, góp phần bảo đảm an toàn cho không gian mạng, Sở Thông tin và Truyền thông đề nghị các sở, ban, ngành, Ủy ban nhân dân các huyện, thành phố triển khai quyết liệt một số khuyến nghị sau:

1. Rà soát, cập nhật, cài đặt phần mềm diệt virus có bản quyền cho các máy chủ, máy trạm của các cơ quan, đơn vị.

2. 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.

3. 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.

4. 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](mailto:ais@mic.gov.vn).

*(Có phụ lục Thông tin về lỗ hổng và hướng dẫn vá lỗi gửi kèm)*

Trân trọng./.

**Nơi nhận:**

- Như trên;
- UBND tỉnh (báo cáo);
- Ban Giám đốc sở (báo cáo);
- Lưu: VT, CNTT.

**KT. GIÁM ĐỐC  
PHÓ GIÁM ĐỐC**

**Nguyễn Văn Hiến**

# PHỤ LỤC THÔNG TIN VỀ LỖ HỔNG

(Kèm theo Công văn số /STTTT-CNTT ngày /9/2020  
của Sở Thông tin và Truyền thông tỉnh Tuyên Quang)

## 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 thực hiện bản vá của Giai đoạn 1

- **Giai đoạn 1:** Thực hiện ngay việc 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