**Phụ lục
Thông tin về lỗ hổng***(kèm theo Công văn số 282/TTCNTT-KTHT ngày 18/9/2020)*

**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 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 thế 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://portal.msrc.microsoft.com/en-US/securi%20tyguidance/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.