**PHỤ LỤC**

**THÔNG TIN VỀ CẢNH BÁO LỖ HỔNG CVE-2021-21985**

*(Kèm theo công văn số /UBND-VHTT ngày 16 tháng 6 năm 2021)*

 **1. Mô tả**

 Theo khuyến cáo bảo mật VMSA 2021-0010 của công ty Vmware vào ngày  25/5/2021, trong đó có thông báo chi tiết đến lỗ hổng CVE-2021-21985 trong  vSphere Client (HTML 5) một thành phần của vCenter Server và Vmware Cloud  Foundation. Lỗ hổng phát sinh do lỗi xác thực thiếu kiểm tra tham số đầu vào  trong tính năng của Virtual SAN Health Check (tính năng này được bật mặc định  trong vCenter Server). Lỗ hổng này thực thi qua cổng 443 (https), cho phép kẻ tấn  công thực hiện các lệnh với đặc quyền cao nhất trong hệ thống và không bị hạn chế  bất kỳ truy cập nào đối với máy chủ cài hệ điều hành vCenter Server. Theo đánh  giá của CVSSv3 mức độ nguy hiểm của CVE-2021-21985 là **9.8** (đặc biệt nghiêm trọng). Đây là nguy cơ có thể gây thiệt hại lớn đến các hệ thống mạng của các cơ  quan, đơn vị đang sử dụng hệ điều hành vCenter Server.

 **2. Các phiên bản bị ảnh hưởng**

 - vCenter Server 6.5

 - vCenter Server 6.7

 - vCenter Server 7.0

 - Cloud Foundation (vCenter Server) 3.x

 - Cloud Foundation (vCenter Server) 4.x

 **3. Bản vá**

 Thông tin về bản vá lỗ hổng theo đường link:

 *https://www.vmware.com/security/advisories/VMSA-2021-0010.html*

 Trong trường hợp đặc biệt nếu không thể vá ngay lập tức, quý cơ quan có thể tắt  tính năng Virtual SAN Health Check tại đường dẫn:

 *https://kb.vmware.com/s/article/83829*

 **4. IOCs**

 Để kiểm tra hệ thống bị tấn công bởi lỗ hổng CVE-2021-21985, có thể kiểm  log trong các thư mục theo đường dẫn mặc định:

 - vCenter Server 6.x và phiên bản cao hơn trên Windows server:  *C:\ProgramData\VMware\vCenterServer\Logs\*

 - vCenter Server Appliance 6.x: */var/log/vmware/*

 - vCenter Server Appliance 6.x flash: */var/log/vmware/vsphere-client*

- vCenter Server Appliance 6.x HTML5: */var/log/vmware/vsphere-ui*

Hoặc theo cấu hình của người dùng có dấu hiệu như sau: 

 **5. Thông tin chi tiết**

 Thông tin chi tiết về lỗ hổng này có tại các đường link dưới đây:

 *- https://www.vmware.com/security/advisories/VMSA-2021-0010.html*

 *-* [*https://blogs.vmware.com/vsphere/2021/05/vmsa-2021-0010.html*](https://blogs.vmware.com/vsphere/2021/05/vmsa-2021-0010.html)

  *- https://core.vmware.com/resource/vmsa-2021-0010-faq*