UBND TỈNH BÌNH THUẬN
SỞ Y TẾ

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

Số: 2543/SYT-VP

Bình Thuận, ngày 05 tháng 7 năm 2021

V/v dự báo sớm nguy cơ tấn công mạng trên diện rộng.

Kính gửi: Các cơ quan, đơn vị trực thuộc.

Sở Y tế nhận được Công văn số 606/STTTT-TTCNTT&TT ngày 30/6/2021 của Sở Thông tin và Truyền thông về việc dự báo sớm nguy cơ tấn công mạng trên diện rộng.

Theo đó, trong thời gian vừa qua, Microsoft có công bố thông tin liên quan tới lỗ hổng bảo mật **(CVE-2021-1675)** được đánh giá có mức độ nguy hiểm cao (7.8/10) ảnh hưởng đến hầu hết các phiên bản của hệ điều hành Windows bao gồm: Windows 10/8.1/7, Windows Server 2019/2016/2012/2008. Lỗ hổng này cho phép đối tượng tấn công leo thang đặc quyền từ tài khoản người dùng thông thường có rất ít quyền . Ngày 08/6/2021, Microsoft đã phát hành bản vá cho lỗ hổng bảo mật nói trên. Tuy nhiên, theo phân tích và đánh giá từ Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) của Cục An toàn thông tin, Bộ Thông tin và Truyền thông đã ghi nhận một số thông tin bổ sung mới cho rằng lỗ hổng bảo mật **(CVE-2021- 1675)** có mức độ nguy hiểm cao hơn thực tế được công bố và **"dự báo sớm"** lỗ hổng này hoàn toàn có thể được tận dụng để tiến hành các chiến dịch tấn công có chủ đích APT lớn trên quy mô rộng trong thời gian ngắn sắp tới vào không gian mạng Việt Nam.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin, Sở Y tế đề nghị các cơ quan, đơn vị trực thuộc thực hiện các nội dung sau:

- Kiểm tra, rà soát và xác định máy chủ, máy trạm sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá bảo mật cho các máy bị ảnh hưởng theo hướng dẫn của Microsoft *(tham khảo hướng dẫn tại phụ lục đính kèm).*

- Tăng cường giám sát hệ thống thông tin và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

Đề nghị các cơ quan, đơn vị trực thuộc khẩn trương triển khai thực hiện./.

- Như trên;
- Cục Công nghệ thông tin- Bộ Y tế;
- Sở Thông tin & Truyền thông tỉnh;
- Lưu: VT, VP, Thành.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Người ký: Sở Y tế tỉnh Bình Thuận
Thời gian ký: 06.07.2021 10:20:15 +07:00

Nguyễn Bá Tòng

Phụ lục

Chi tiết lỗ hổng và hướng dẫn khắc phục

(Kèm theo Công văn số 926/SYT-VP ngày 25/3/2021 của Sở Y tế)

STT	Tên lỗ hổng	Sản phẩm ảnh hưởng	Phiên bản	Phiên bản đã vá lỗ hổng	Hướng dẫn vá lỗ hổng
1	VSphere Client (HTML5) chứa lỗ hổng thực thi mã từ xa trong plugin vCenter Server (CVE-2021-21972)	vCenter Server	6.5	6.5 U3n	https://kb.vmware.com/s/article/82374
		vCenter Server	6.7	6.7 U3l	https://kb.vmware.com/s/article/82374
		vCenter Server	7.0	7.0 U1c	https://kb.vmware.com/s/article/82374
		Cloud Foundation (vCenter Server)	3.x	3.10.1.2	https://kb.vmware.com/s/article/82374
		Cloud Foundation (vCenter Server)	4.x	4.2	https://kb.vmware.com/s/article/82374
2	ESXi OpenSLP chứa lỗ hổng tràn heap (heap-overflow) (CVE-2021-21974)	ESXi	6.5	ESXi650-202102101-SG	https://kb.vmware.com/s/article/76372
		ESXi	6.7	ESXi670-202102401-SG	https://kb.vmware.com/s/article/76372
		ESXi	7.0	ESXi70U1c-17325551	https://kb.vmware.com/s/article/76372
		Cloud Foundation (ESXi)	3.x		https://kb.vmware.com/s/article/76372
		Cloud Foundation (ESXi)	4.x	4.2	https://kb.vmware.com/s/article/76372

Phụ lục
Chi tiết lỗ hổng và hướng dẫn khắc phục
(Kèm theo Công văn số 228*/STTTT-TTCNTT&TT ngày 23/3/2021 của Sở TT&TT)*

STT	Tên lỗ hổng	Sản phẩm ảnh hưởng	Phiên bản	Phiên bản đã vá lỗ hổng	Hướng dẫn vá lỗ hổng
1	VSphere Client (HTML 5) chứa lỗ hổng thực thi mã từ xa trong plug in vCenter Server (CVE-2021-21972)	vCenter Server	6.5	6.5 U3n	https://kb.vmware.com/s/article/82374
vCenter Server	6.7	6.7 U3l	https://kb.vmware.com/s/article/82374		

vCenter Server	7.0	7.0 U1c	https://kb.vmware.com/s/article/82374		
Cloud Foundation (vCenter Server)	3.x	3.10.1.2	https://kb.vmware.com/s/article/82374		
Cloud Foundation (vCenter Server)	4.x	4.2	https://kb.vmware.com/s/article/82374		
2	ESXi OpenSLP chứa lỗ hổng tràn heap (heap overflow) (CVE-2021-21974)	ESXi	6.5	ESXi650-202102101-SG	https://kb.vmware.com/s/article/76372

ESXi	6.7	ESXi670-202102401-SG	https://kb.vmware.com/s/article/76372		
ESXi	7.0	ESXi70U1c-17325551	https://kb.vmware.com/s/article/76372		
Cloud Foundation (ESXi)	3.x	https://kb.vmware.com/s/article/76372			
Cloud Foundation (ESXi)	4.x	4.2	https://kb.vmware.com/s/article/76372		