UBND TỈNH GIA LAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 1717/STTTT-CNTT
V/v cảnh báo 19 lỗ hổng bảo mật mới trong VMware

Gia Lai, ngày 27 tháng 9 năm 2021

Kính gửi:

- Công an tỉnh;
- Bộ Chỉ huy Quân sự tỉnh;
- Bộ Chỉ huy Bộ đội biên phòng tỉnh;
- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn đại biểu Quốc hội và Hội đồng nhân dân tỉnh;
- Văn phòng Ủy ban Mặt trận tổ quốc Việt Nam tỉnh;
- Các sở, ban, ngành thuộc tỉnh;
- Các hội, đoàn thể tỉnh;
- Ủy ban nhân dân các huyện, thị xã, thành phố;
- Trung tâm Công nghệ thông tin và Truyền thông tỉnh Gia Lai.

Ngày 21/9/2021 vừa qua, VMware vừa công bố 19 lỗ hổng bảo mật ảnh hưởng đến VMware vCenter Server phiên bản 7.0/6.7/6.5 và VMware vClound Foundation phiên bản 4.3.1/3.10.2.2. Trong đó đáng chú ý:

- Lỗ hổng bảo mật (CVE-2021-22005) có mức ảnh hưởng nghiêm trọng (điểm CVSS:9.8), cho phép đối tượng tấn công không cần xác thực có thể thực thi mã tùy ý.

- 11 lỗ hổng bảo mật (CVE-2021-21991, CVE-2021-22006, CVE-2021-22011, CVE-2021-22015, CVE-2021-22012, CVE-2021-22013, CVE-2021-22016, CVE-2021-22017, CVE-2021-22014, CVE-2021-22018, CVE-2021-21992) có mức ảnh hưởng cao, cho phép đối tượng tấn công khai thác dưới nhiều hình thức khác nhau như thu thập thông tin, tấn công leo thang, tấn công từ chối dịch vụ,…. Trong đó có 07 lỗ hổng bảo mật (CVE-2021-22006, CVE-2021-22011, CVE-2021-22012, CVE-2021-22013, CVE-2021-22016, CVE-2021-22017, CVE-2021-22018) có thể khai thác mà không cần xác thực.

Các sản phẩm của VMware được sử dụng khá phổ biến trong các cơ quan tổ chức, doanh nghiệp; đã và đang là mục tiêu nhằm đến của các đối tượng tấn công mạng; đặc biệt là các nhóm chuyên thực hiện tấn công APT.

Thực hiện khuyến nghị của Cục An toàn thông tin tại Công văn số 1286/CATTT-NCSC ngày 22/9/2021 về việc 19 lỗ hổng bảo mật mới trong VMware; Sở Thông tin và Truyền thông đề nghị các đơn vị, địa phương kiểm tra, rà soát, khắc phục kịp thời hổng bảo mật mới trong VMware, cụ thể như sau:

1. Kiểm tra, rà soát và xác định hệ thống thông tin có khả năng bị ảnh hưởng bởi lỗ hổng bảo mật như trên để có phương án xử lý, khắc phục lỗ hổng.

Thực hiện cập nhật bản vá phù hợp với phiên bản sản phẩm VMware đang sử dụng (*Hướng dẫn chi tiết trong Phụ lục đính kèm*)

2. Tăng cường giám sát 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.

Sở Thông tin và Truyền thông tỉnh Gia Lai đề nghị các đơn vị, địa phương phối hợp, triển khai thực hiện./.

Nơi nhận:
- Như trên;
- UBND tỉnh (báo cáo);
- Cục An toàn thông tin (báo cáo);
- Lưu: VT, P. CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X H C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH GIA LAI

Đặng Quang Khanh

Phụ lục:

THÔNG TIN VỀ 19 LỖ HỔNG BẢO MẬT MỚI TRONG VMWARE VÀ HƯỚNG DẪN XỬ LÝ, KHẮC PHỤC LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số : 1717/STTTT-CNTT ngày 27 tháng 9 năm 2021 của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hổng bảo mật:

- Mô tả: Lỗ hổng ảnh hưởng đến sản phẩm camera IP Hikvision, cho phép đối tượng tấn công thực thi mã từ xa mà không cần xác thực, từ đó chiếm toàn quyền kiểm soát thiết bị và có thể truy cập và tấn công mạng nội bộ của mục tiêu.

- Điểm CVSS: 9.8 (nghiêm trọng)

- Ảnh hưởng:

Số TT	TÊN LỖ HỔNG	MÔ TẢ
1	CVE-2021-22005	- Lỗ hổng tồn tại trong dịch vụ Analytics của vCenter Server, cho phép đối tượng tấn công không cần xác thực thực thi mã tùy ý. - Điểm CVSS: 9.8 (nghiêm trọng)
2	CVE-2021-21991	- Lỗ hổng trong vCenter Server, cho phép đối tượng tấn công đã xác thực thực hiện tấn công leo thang. - Điểm CVSS: 8.8 (cao)
3	CVE-2021-22006	- Lỗ hổng trong vCenter Server, cho phép đối tượng tấn công không cần xác thực bypass proxy, truy cập trái phép - Điểm CVSS: 8.3 (cao)
4	CVE-2021-22011	- Lỗ hổng trong vCenter Server Content Library, cho phép đối tượng tấn công không cần xác thực truy cập một số API. - Điểm CVSS: 8.1 (cao)
5	CVE-2021-22015	- Lỗ hổng trong vCenter Server Content Library, cho phép đối tượng tấn công đã xác thực thực hiện tấn công leo thang. - Điểm CVSS: 7.8 (cao)
6	CVE-2021-22012	- Lỗ hổng trong vCenter Server, cho phép đối tượng tấn công không cần xác thực truy cập một số API và thu thập thông tin. - Điểm CVSS: 7.5 (cao)
7	CVE-2021-22013	- Lỗ hổng trong vCenter Server, cho phép đối tượng tấn công không cần xác thực thu thập thông tin từ một số API. - Điểm CVSS: 7.5 (cao)

Số TT	TÊN LỖ HỔNG	MÔ TẢ
8	CVE-2021-22016	- Lỗ hổng trong vCenter Server, cho phép đối tượng tấn công không cần xác thực thực hiện tấn công XSS. - Điểm CVSS: 7.5 (cao)
9	CVE-2021-22017	- Lỗ hổng tồn tại trong vCenter Server, cho phép đối tượng tấn công không cần xác thực thực hiện tấn công XSS - Điểm CVSS: 7.3 (cao)
10	CVE-2021-22014	- Lỗ hổng tồn tại trong VAMI (Virtual Appliance Management Infrastructure), cho phép đối tượng có quyền cao trên hệ thống thực hiện tấn công thực thi mã tùy ý. - Điểm CVSS: 7.2 (cao)
11	CVE-2021-22018	- Lỗ hổng tồn tại trong Vmware vSphere Lifecycle Manager plug-in, cho phép đối tượng tấn công không cần xác thực thực hiện xóa tệp tùy ý. - Điểm CVSS: 6.5 (cao)
12	CVE-2021-21992	- Lỗ hổng tồn tại trong quá trình xử lý XML của vCenter Server, cho phép đối tượng tấn công đã xác thực thực hiện tấn công từ chối dịch vụ. - Điểm CVSS: 6.5 (cao)
13	CVE-2021-22007	- Lỗ hổng tồn tại trong dịch vụ Analytics của vCenterServer, cho phép đối tượng tấn công đã xác thực thu thập thông tin nội bộ của máy chủ. - Điểm CVSS: 5.5 (trung bình)
14	CVE-2021-22019	- Lỗ hổng tồn tại trong dịch vụ VAPI (vCenter API) của vCenterServer, cho phép đối tượng tấn công không cần xác thực thực hiện tấn công từ chối dịch vụ. - Điểm CVSS: 5.3 (trung bình)
15	CVE-2021-22009	- Lỗ hổng tồn tại trong dịch vụ VAPI (vCenter API) của vCenterServer, cho phép đối tượng tấn công không cần xác thực thực hiện tấn công từ chối dịch vụ. - Điểm CVSS: 5.3 (trung bình)
16	CVE-2021-22010	- Lỗ hổng tồn tại trong dịch vụ VPXD (Virtual Provisioning X Daemon) của vCenterServer, cho phép đối tượng tấn công không cần xác thực thực hiện tấn công từ chối dịch vụ. - Điểm CVSS: 5.3 (trung bình)
17	CVE-2021-22008	- Lỗ hổng tồn tại trong dịch vụ VAPI (vCenter API) của vCenterServer, cho phép đối tượng tấn

Số TT	TÊN LỖ HỔNG	MÔ TẢ
		công không cần xác thực thực hiện tấn công thu thập thông tin. - Điểm CVSS: 5.3 (trung bình)
18	CVE-2021-22020	- Lỗ hổng tồn tại trong dịch vụ Analytics của vCenterServer, cho phép đối tượng tấn công đã xác thực thực hiện tấn công từ chối dịch vụ. - Điểm CVSS: 5.0 (trung bình)
19	CVE-2021-21993	- Lỗ hổng tồn tại trong vCenter Server Content Library, cho phép đối tượng tấn công đã xác thực thực hiện tấn công SSRF. - Điểm CVSS: 4.3 (trung bình)

- Ảnh hưởng: vCenter Server phiên bản 7.0/6.7/6.5 và vClound Foundation phiên bản 4.3.1/3.10.2.2

2. Hướng dẫn khắc phục:

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng bảo mật nói trên theo hướng dẫn của hãng. Thông tin các bản cập nhật:

https://www.vmware.com/security/advisories/VMSA-2021-0020.html

3. Nguồn tham khảo:

https://www.vmware.com/security/advisories/VMSA-2021-0020.html