BẢN TIN NỘI BỘ

CẬP NHẬT VỀ AN TOÀN THÔNG TIN VÀ CẢNH BÁO LỖ HỔNG BẢO MẬT

1. Microsoft kêu gọi người dùng Windows cài đặt bản vá bảo mật khẩn cấp

Theo TechCrunch, Microsoft cho biết lỗ hổng bảo mật trong một số phiên bản Internet Explorer có thể cho phép kẻ tấn công chạy mã độc từ xa trên thiết bị bị ảnh hưởng. Người dùng có thể bị lây nhiễm lén lút bằng cách truy cập trang web độc hại hoặc bị lừa nhấp vào liên kết trong email.

Cũng theo Microsoft, một kẻ tấn công khai thác thành công lỗ hổng này có thể kiểm soát hệ thống bị ảnh hưởng. Mặc dù chi tiết về lỗ hổng chưa được công khai nhưng Microsoft cho biết nó đang được khai thác tích cực.

Dữ liệu gần đây từ NetMarketShare cho thấy, hơn 7% lượng người dùng trình duyệt đang chạy các phiên bản bị ảnh hưởng bởi lỗ hổng, gồm Internet Explorer 9, 10 và 11. Tất cả phiên bản Windows đang nằm trong danh mục được hỗ trợ đều bị ảnh hưởng, gồm Windows 7, 8.1 và 10, cũng như một số phiên bản Windows Server. Hầu hết người dùng có thể cài đặt các bản vá bằng Windows Update.

Microsoft cũng đã đưa ra một bản sửa lỗi cho trình quét phần mềm độc hại tích hợp Windows Defender, vốn tồn tại lỗ hổng mà nếu bị khai thác có thể đã gây ra tình trạng từ chối dịch vụ (DDoS) dẫn đến ứng dụng không hoạt động.

Được biết, thật hiếm khi Microsoft phát hành các bản vá bảo mật khẩn cấp ngoài chu kỳ vá hằng tháng điển hình. Công ty thường phát hành các bản sửa lỗi bảo mật vào thứ ba của tuần thứ hai mỗi tháng, còn được gọi là Patch Tuesday, nhưng họ cũng sẽ phát hành bản sửa lỗi cho các lỗ hổng đáng kể nếu phát hiện một cuộc tấn công mạnh nhằm vào nó.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng hệ điều hành Windows cần cập nhật các bản vá mới nhất để đảm bảo an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/microsoft-keu-goi-nguoi-dung-windows-cai-dat-ban-va-bao-mat-khan-cap-1129962.html

2. Cảnh báo lỗ hổng bảo mật trên Jenkins giúp hacker chiếm quyền điều khiển máy tính của doanh nghiệp

Ông Trương Đức Lượng – Tổng Giám đốc Công ty cổ phần An ninh mạng Việt Nam (VSEC) cho biết VSEC đã phát đi cảnh báo lỗ hổng bảo mật nghiêm trọng trên ứng dụng mã nguồn mở Jenkins, có thể gây ảnh hưởng nghiêm trọng tới hệ thống máy tính của các doanh nghiệp Việt Nam.

Theo VSEC, lỗ hổng có mã CVE-2019-10392, được chuyên gia bảo mật người Hà Lan Francesco Soncina phát hiện. Với lỗ hổng được đánh giá mức độ nguy hiểm 8/10 này, hacker sẽ dễ dàng chiếm được quyền điều khiển máy chủ, kiểm soát toàn bộ hệ thống thông tin của doanh nghiệp và thực hiện các hoạt động trái phép.

Các chuyên gia bảo mật VSEC đã nhanh chóng tiến hành nghiên cứu và công bố cách thức hoạt động của lỗ hổng. Cụ thể, để khai thác thành công hacker cần tài khoản người dùng cùng quyền cấu hình "Job/Configure (USE_ITEM)" và "Git Client

Plugin" từ phiên bản 2.8.4 trở về trước. "Việc không kiểm soát giá trị đầu vào tại tham số Repository URL trong Git Client Plugin chính là mấu chốt giúp hacker thực thi mã lệnh trái phép trên máy chủ", chuyên gia VSEC cho hay.

Chia sẻ với ICTnews về mức độ ảnh hưởng của lỗ hổng bảo mật ứng dụng mã nguồn mở Jenkins đối với các doanh nghiệp Việt Nam, chuyên gia VSEC cho biết, hệ thống CI (Continuous Integration) là một trong những hệ thống phổ biến nhất tại các doanh nghiệp công nghệ Việt Nam, 80% doanh nghiệp có hệ thống CI đều sử dụng ứng dụng Jenkins để giúp tự động hoá trong nhiều công đoạn phát triển phần mềm và các sản phẩm có nhiều người dùng như mạng xã hội, ứng dụng chát hay các trang thương mại điện tử.

Khai thác lỗ hổng bảo mật trên Jenkins, các hacker sẽ dễ dàng chiếm được quyền điều khiển máy chủ, kiểm soát toàn bộ hệ thống thông tin quan trọng của doanh nghiệp và thực hiện các hoạt động trái phép như đánh cắp thông tin, phát tán dữ liệu mật, thực hiện các hành vi giao dịch trái phép từ tài khoản khách hàng…

Chuyên gia VSEC cho biết, theo thống kê, hiện có hơn 200.000 máy chủ cài đặt Jenkins phiên bản bị lỗi công khai trên Internet.

Do mức độ nghiêm trọng của lỗ hổng, VSEC khuyến cáo các tổ chức, doanh nghiệp cập nhật Git Client Plugin của Jenkins phiên bản mới nhất và nhanh nhất có thể. Ngoài ra, các doanh nghiệp cần hạn chế công khai những hệ thống đang sử dụng trong mạng nội bộ, cấu hình Whitelist các IP được truy cập vào các hệ thống quan trọng, đồng thời cài đặt mật khẩu mạnh đối với tài khoản hệ thống kể cả tài khoản có quyền hạn thấp.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người quản trị cần cập nhật Git Clinet Plugin của Jenkins phiên bản mới nhất để đảm bảo an toàn thông tin.

Link tham khảo: https://ictnews.vn/cntt/bao-mat/canh-bao-lo-hong-bao-mat-tren-jenkins-giup-hacker-chiem-quyen-dieu-khien-may-tinh-cua-doanh-nghiep-190749.ict

3. VMware vá 6 lỗ hổng trong nhiều sản phẩm

VMware vừa tung bản vá cho các lỗi thực thi mã, chèn lệnh (command injection), tiết lộ thông tin và tấn công từ chối dịch vụ (DoS) trong các sản phẩm của hãng bao gồm ESXi, vCenter Server, Workstation, Fusion, VMRC và Horizon Client.

Đầu tiên là 4 lỗi ảnh hưởng đến ESXi và vCenter Server. Nghiêm trọng nhất là lỗ hổng CVE-2019-5532 và CVE-2019-5534 để lộ thông tin ở mức độ cao ảnh hưởng đến vCenter Server.

Các lỗ hổng được VMware phân loại ở mức độ "quan trọng", liên quan đến các máy ảo Open Virtualization Format (OVF) có thể cho phép kẻ xấu có quyền truy cập thông tin đăng nhập được sử dụng để triển khai OVF. Những thông tin đăng nhập này thường được dành cho các tài khoản root của máy ảo.

Người dùng cũng đã được thông báo để cập nhật bản vá cho lỗ hổng chèn lệnh Busybox ảnh hưởng đến ESXi, cho phép kẻ tấn công lừa quản trị viên thực thi các lệnh shell bằng việc cung cấp cho họ một file độc hại.

VMware cũng xử lý lỗi trong ESXi và vCenter Server vSphere cho phép kẻ tấn công cục bộ hoặc man-in-the-middle (MitM) chiếm quyền kiểm soát của một VM console (dòng lệnh để chạy máy ảo) nếu người dùng đăng xuất khi phiên đăng nhập hết thời gian.

Bên cạnh đó, VMware cũng đưa ra khuyến cáo về hai lỗ hổng khác. Một trong số đó là CVE-2019-5527, có mức độ nghiêm trọng cao liên quan đến thiết bị âm thanh ảo được sử dụng bởi ESXi, Workstation, Fusion, VMRC và Horizon Client. Thành phần này bị ảnh hưởng bởi lỗi use-after-free (cho phép thực thi mã từ xa nếu người dùng tương tác với nội dung độc hại), có thể bị khai thác bởi kẻ tấn công cục bộ không có quyền quản trị truy cập đến máy khách để thực thi mã tùy ý trên máy host.

Lỗ hổng này chỉ có thể bị khai thác nếu khâu xử lý âm thanh hợp lệ không có kết nối.

Lỗ hổng thứ hai được đánh giá ở mức "trung bình" ảnh hưởng đến Workstation ở bất kỳ nền tảng nào và Fusion trên macOS, có thể bị khai thác dẫn đến tấn công DoS bằng cách gửi các gói IPv6 tự tạo từ máy khách đến hệ thống VMware Network Address Translation (NAT).

Khuyến nghị:

Phòng ATTT khuyến nghị: Người quản trị và người sử dụng các dịch vụ VMware cần cập nhật bản vá mới nhất để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/vmware-va-6-lo-hong-trong-nhieu-san-pham.12732/

TECHNICAL PAGES:

1. Chi tiết về thông tin một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam trong tuần, cụ thể như sau:

STT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Microsoft	CVE-2019-1208 CVE-2019-1221 CVE-2019-1246 …	Nhóm 79 lỗ hổng trên các sản phẩm, phần mềm của Microsoft (Office, IE, Windows 7/10, Microsoft Edge…) cho phép đối tượng tấn công thực hiện nhiều hình thức tấn công khác nhau bao gồm: thu thập thông tin, tấn công từ chối dịch vụ, chèn và thực thi mã từ xa, tấn công leo thang. Nhiều lỗ hổng có điểm CVSS cao (9.3, 7.6)	Đã có thông tin xác nhận và bản vá.
2	Adobe	CVE-2019-8069 CVE-2019-8070 CVE-2019-8076	Nhóm 03 lỗ hổng trên sản phẩm của Adobe (Flash Player, Adobe application manage) cho phép đối tượng tấn công chèn và thực thi mã lệnh 02 Lỗ hổng trên Flash Player có điểm CVSS là 10.0 Ảnh hưởng đến nhiều phiên bản Adobe.	Đã có thông tin xác nhận và bản vá
3	WordPress	CVE-2019-16217 CVE-2019-16218 CVE-2019-16219 …	Nhóm 18 lỗ hổng trên nhiều thành phần của WordPress cho phép đối tượng tấn công khai thác lỗi XSS, SQL injection, truy cập trái phép vào thông tin người dùng trên hệ thống hay chuyển hướng người dùng đến trang web độc hại	Đã có thông tin xác nhận và bản vá
4	Android	CVE-2019-9461 CVE-2018-6240 CVE-2019-9345 …	Nhóm 32 lỗ hổng trên hệ điều hành Android cho phép đối tượng tấn công thực hiện thu thập thông tin, tấn công leo thang qua nhiều thành phần khác nhau	Đã có thông tin xác nhận và bản vá
5	Apache	CVE-2018-17200 CVE-2019-0189 CVE-2019-10074	Nhóm 06 lỗ hổng trên một số sản phẩm, phần mềm của Apache (như OFBiz, Solr, Apache Traffic Control) cho	Đã có thông tin xác nhận và bản vá

			phép đối tượng tấn công khai thác lỗi Stored XSS, truy cập trái phép vào hệ thống mà chỉ cần thông tin username.	
6	Dlink	CVE-2019-10891 CVE-2019-10892 CVE-2019-16190 ….	Nhóm 03 lỗ hổng trên một số phiên bản firmware của thiết bị Dlink (DIR-806, DIR-868L REVB) cho phép đối tượng tấ công chèn và thực thi lệnh độc hại qua nhiều thành phần khác nhau 02 lỗ hổng có điểm CVSS là 10.0	Đã có thông tin xác nhận và bản vá

2. Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam

STT	**Tên miền/IP**
1	disorderstatus.ru
2	differentia.ru
3	atomictrivia.ru
4	soplifan.ru
5	6kie9jomo.ru
6	xjpakmdcfuqe.com
7	xdqzpbcgrvkj.ru
8	www.cityofangelsmagazine.com
9	dklxjmtbnmn.info
10	morphed.ru

3. Các cán bộ kỹ thuật đầu mối về ATTT cần thực hiện:
- Xử lý các lỗ hổng phát hiện tại bảng 1 (nếu có).
- Chặn, xử lý các truy nhập tới các tên miền độc hại tại bảng 2.