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

1. Cảnh báo chiến dịch phát tán mã độc mã hóa dữ liệu tống tiền W32.WeakPass nhắm vào các Server tại Việt Nam

Chiều 14/2, Hệ thống giám sát virus của Bkav vừa phát đi cảnh báo đang có một chiến dịch tấn công có chủ đích của các hacker nước ngoài nhằm vào các Server Public của Việt Nam. Đặc biệt, trong chiến dịch này, hacker chỉ tấn công các máy chủ, khác với các mã độc mã hóa dữ liệu trước đây thường nhắm vào các máy trạm.

Các địa chỉ phát động tấn công của hacker xuất phát từ Nga, châu Âu và châu Mỹ. Rất nhiều cơ quan, tổ chức tại Việt Nam đã bị hacker tấn công, xâm nhập máy chủ, sau đó thực hiện mã hóa toàn bộ dữ liệu trên server. Hiện chưa có con số thống kê đầy đủ, nhưng theo ước tính của Bkav, đến cuối buổi chiều 14/2 số nạn nhân có thể đã lên đến hàng trăm cơ quan, tổ chức.

Cách thức tấn công của hacker là rà quét các Server cài hệ điều hành Windows của các cơ quan, tổ chức tại Việt Nam, dò mật khẩu của những server này bằng cách sử dụng từ điển để thử từng mật khẩu (brute force). Nếu dò thành công, hacker sẽ thực hiện đăng nhập từ xa qua dịch vụ remote desktop, cài mã độc mã hóa tống tiền lên máy của nạn nhân.

Các dữ liệu sẽ bị mã hóa bao gồm các file văn bản, file tài liệu, file cơ sở dữ liệu, file thực thi… Nạn nhân muốn lấy lại dữ liệu phải trả tiền chuộc cho hacker. Hacker không công bố số tiền nạn nhân phải trả như các mã độc mã hóa tống tiền thông thường, mà yêu cầu nạn nhân phải liên lạc qua email để trao đổi, thỏa thuận cụ thể. Theo ghi nhận của Bkav thì mỗi máy chủ bị mã hóa dữ liệu, hacker đang để lại một email khác nhau để liên hệ.

Hiện tại Bkav đã cập nhật mẫu nhận diện mã độc mã hóa dữ liệu W32.WeakPass vào các phiên bản phần mềm diệt virus Bkav, bao gồm cả bản miễn phí, các quản trị có thể tải Bkav để quét và kiểm tra cho các máy chủ. Tuy nhiên, để phòng chống triệt để loại tấn công này, Bkav khuyến cáo quản trị viên cần lên kế hoạch rà soát ngay toàn bộ các máy chủ đang quản lý, đặc biệt là các máy chủ thuộc dạng public ra ngoài Internet, cần đặt mật khẩu mạnh cho máy chủ, đồng thời tắt dịch vụ remote desktop cho máy chủ nếu không thực sự cần thiết. Trong trường hợp vẫn cần phải duy trì remote desktop, cần giới hạn quyền truy cập, cấu hình chỉ cho các IP cố định, biết trước được phép remote vào.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người quản trị cần kiểm tra kỹ các máy chủ sử dụng hệ điều hành Windows, đặt mật khẩu mạnh và đổi mật khẩu theo định kỳ, tắt dịch vụ remote desktop nếu không cần thiết. Trong trường hợp cần remote desktop, cần giới hạn quyền truy nhập, chỉ cho các IP cố định được, biết trước được remote.

Link tham khảo: https://whitehat.vn/threads/canh-bao-chien-dich-phat-tan-ma-doc-ma-hoa-du-lieu-tong-tien-w32-weakpass-nham-vao-cac-server-tai-viet-nam.11976/

2. Microsoft vá 77 lỗi trong tháng 2/2019

Microsoft đã phát hành bản vá thứ hai trong năm nay để vá tổng cộng 77 lỗ hổng bảo mật trong các hệ điều hành Windows và các sản phẩm khác, 20 trong số đó được đánh giá là nghiêm trọng, 54 mức độ nghiêm trọng và 3 mức độ nghiêm trọng.

Cập nhật bảo mật tháng 2 giải quyết các lỗi trong Adobe Flash Player, Internet Explorer, Edge, Windows, MS Office và Office Services và Web Apps, ChakraCore, .NET Framework, Exchange Server, Visual Studio, Azure IoT SDK, Dynamics, Team Foundation Server và Visual Studio Code.

Bốn trong số các lỗ hổng bảo mật được vá trong tháng này đã được thông báo, và một trong số đó đang được khai thác trong tự nhiên.

Lỗ hổng được đánh giá là quan trọng và nằm trong cách Internet Explorer xử lý các đối tượng trong bộ nhớ.

Kẻ tấn công có thể lừa nạn nhân truy cập một trang web được chế tạo đặc biệt và khai thác lỗ hổng này, Lỗ hổng CVE-2019-0676 dẫn đến tiết lộ thông tin.

Một trong những lỗ hổng được công khai nhưng chưa được khai thác là CVE-2019-0636 và được đánh giá là quan trọng, liên quan đến lỗ hổng thông tin trong hệ điều hành Windows có thể cho phép kẻ tấn công đọc nội dung của tệp trên đĩa.

"Một lỗ hổng thông tin tồn tại khi Windows xử lý không đúng tệp tin ", Microsoft nói khuyến cáo". Để khai thác lỗ hổng, kẻ tấn công sẽ phải đăng nhập vào hệ thống bị ảnh hưởng và chạy một ứng dụng được chế tạo đặc biệt."

Hầu hết các lỗ hổng được xếp mức nghiêm trọng đều dẫn đến các cuộc tấn công thực thi mã từ xa và chủ yếu ảnh hưởng đến các phiên bản khác nhau của phiên bản Windows 10 và Server.

Mặc dù chưa được khai thác công khai, các lỗ hổng thực thi mã từ xa quan trọng trong SharePoint (CVE-2019-0594 và CVE-2019-0604) và Máy chủ DHCP Windows (CVE-2019-0626) nguy hiểm hơn, vì việc khai thác thành công các lỗ hổng này có thể cho phép kẻ tấn công chạy mã tùy ý và kiểm soát máy chủ.

Trong khi một số lỗ hổng được xếp hạng quan trọng cũng có thể là nguyên nhân của các cuộc tấn công thực thi mã từ xa, một số lỗ hổng khác cho phép nâng cao đặc quyền, tiết lộ thông tin, bỏ qua tính năng bảo mật và lỗ hổng giả mạo.

Người dùng và quản trị viên hệ thống được khuyến nghị áp dụng các bản vá bảo mật mới nhất càng sớm càng tốt để ngăn chặn tin tặc và tội phạm mạng không kiểm soát hệ thống của họ.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng và quản trị hệ thống cần áp dụng các bản vá và bảo mật mới nhất ngay lập tức để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/microsoft-va-77-loi-trong-thang-2-2019.11974/

3. Lỗ hổng Dirty Sock cho phép kẻ tấn công giành quyền truy cập root trên các hệ thống Linux

Sau Dirty COW vào năm 2016, giờ các hệ thống Linux phải lo lắng về Dirty Sock.

Một nhà nghiên cứu bảo mật vừa công bố minh chứng (PoC) về một lỗ hổng chủ yếu ảnh hưởng Ubuntu, nhưng cũng tác động đến các bản phân phối Linux khác.

Canonical, công ty đứng sau hệ điều hành Ubuntu, đã phát hành một bản vá (USN-3887-1) cho vấn đề này vào ngày hôm qua, trước khi tiết lộ đầy đủ về lỗ hổng.

Lỗ hổng được phát hiện vào cuối tháng 1 bởi Chris Moberly, một nhà nghiên cứu bảo mật của Shenanigans Labs.

Lỗ hổng, mà Moberly gọi là Dirty Sock, không cho phép tin tặc xâm nhập từ xa vào các máy tồn tại lỗ hổng, nhưng một khi kẻ tấn công đã vào được hệ thống, thì sẽ dễ dàng leo lên quyền cao nhất, kiểm soát toàn bộ hệ điều hành.

Theo thuật ngữ kỹ thuật, Dirty Sock là một lỗ hổng leo thang đặc quyền cục bộ cho phép tin tặc tạo tài khoản cấp root.

Lỗ hổng thực tế không nằm trong hệ điều hành Ubuntu, mà trong daemon Snapd được bao gồm theo mặc định trong tất cả các phiên bản Ubuntu gần đây, và trong một số bản phân phối Linux khác.

Snapd là một daemon (trình nền) quản lý "snaps", định dạng đóng gói ứng dụng mới được Canonical phát triển và sử dụng cho các ứng dụng Ubuntu từ năm 2014. Snapd cho phép người dùng tải xuống và cài đặt ứng dụng ở định dạng tệp .snap.

Moberly cho biết Snapd để lộ một máy chủ REST API cục bộ mà các gói snap (và Ubuntu Snap Store chính thức) tương tác trong quá trình cài đặt các ứng dụng mới (snaps).

Theo nhà nghiên cứu, ông đã xác định một cách để vượt qua các hạn chế kiểm soát truy cập được áp dụng trên máy chủ API này và giành quyền truy cập vào tất cả các chức năng API, bao gồm cả các chức năng bị hạn chế với người dùng root.

Minh chứng (PoC) mà Moberly công bố trên GitHub bao gồm hai khai thác mẫu có thể được sử dụng để lợi dụng API này và tạo tài khoản cấp root mới.

Mã độc để khai thác lỗ hổng này (cũng được theo dõi là CVE-2019-7304) có thể được chạy trực tiếp trên máy chủ bị lây nhiễm hoặc có thể bị ẩn trong các gói snap độc hại - một số được biết là đã từng xuất hiện trên Ubuntu Snap Store.

Các phiên bản Snapd 2.28 đến 2.37 đều dễ bị tấn công Dirty Sock. Moberly đã báo cáo vấn đề này với Canonical, nhà phát triển của Snapd. Canonical đã phát hành Snapd phiên bản 2.37.1 trong tuần này để giải quyết vấn đề này.

Đồng thời, Canonical cũng phát hành các bản cập nhật an ninh cho hệ điều hành Ubuntu Linux, là nơi mà gói Snapd được phát triển và bao gồm và bật theo mặc định.

Các bản phân phối Linux khác sử dụng Snapd cũng đưa ra các bản cập nhật an ninh, như Debian, Arch Linux, OpenSUSE, Solus và Fedora.

Theo các chuyên gia Bkav, người dùng Snapd phiên bản dưới 2.37.1 cần nhanh chóng cập nhật lên phiên bản mới nhất.

Cách kiểm tra phiên bản snapd hiện tại của hệ thống:

+ Chạy lệnh sau trong terminal:

snap --version

+ Nếu thấy có dòng "snapd 2.37.1" thì 2.37.1 là phiên bản hiện tại của snapd. Nếu phiên bản snapd là 2.37.1 hoặc cao hơn thì hệ thống an toàn. Ngược lại cần tiến hành cập nhật snapd lên phiên bản mới nhất.

Cập nhật bản vá:

sudo apt-get update && apt-get upgrade

Khuyến nghị:

Phòng ATTT khuyến nghị: Người quản trị hệ thống cần cập nhật phiên bản mới nhất của Snapd để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/lo-hong-dirty-sock-cho-phep-ke-tan-cong-gianh-quyen-truy-cap-root-tren-cac-he-thong-linux.11975/

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	Apache Netbeans	CVE-2018-17191 …	Lỗ hổng trong Apache Netbeans (Môi trường phát triển các ứng dụng Java) cho phép đối tượng tấn công chèn và thực thi mã lệnh. Có thể cập nhật lên Netbean10.0	Đã có thông tin xác nhận và bản vá
2	F5	CVE-2018-15334 CVE-2018-15335 CVE-2018-17539	Nhóm 04 lỗ hổng trên một số sản phẩm của F5 (BIG-IP APM) cho phép đối tượng tấn công thực hiện cho phép đối tượng tấn công khai thác lỗi CSRF, tấn công từ chối dịch vụ, người dùng Guest có thể truy cập và xóa tập tin tùy ý bao gồm cả những tập tin cấu hình.	Đã có thông tin xác nhận và bản vá
3	Fasterxml Jackson	CVE-2018-14718 CVE-2018-19360 CVE-2018-14720 ...	Nhóm 07 lỗ hổng trên bộ thư viện Fasterxml Jackson cho phép đối tượng tấn công thực hiện mã lệnh tùy ý thông qua một số thành phần (slf4j-ext, blaze-ds-opt, -core jars), khai thác lỗi SSRF (trong thành phần axis2-jaxws)	Đã có thông tin xác nhận
4	Foxit	CVE-2019-5007 CVE-2019-5006 CVE-2019-5005	Nhóm 03 lỗ hổng trên Foxit Foxit Reader và PhantomPDF (phiên bản cho hệ điều hành Windows) cho phép đối tượng tấn công khai thác lỗi tràn bộ đệm	Đã có thông tin xác nhận và bản vá
5	FreeBSD	CVE-2018-17161	Lỗ hổng trong một số phiên bản của hệ điều hành FreeBSD cho phép đối tượng tấn công khai thác lỗi tràn bộ đệm để chèn và thực thi mã lệnh.	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	q4dgp6xv.ru
5	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
6	xjpakmdcfuqe.com
7	9lnbo2e3.ru
8	www.cityofangelsmagazine.com
9	dqrzxapnw.info
10	caarmelcollege.org

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.