BẢN TIN NỘI BỘ

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

1. Ra mắt cộng đồng kết nối hacker mũ trắng và chuyên gia bảo mật

Vietnam Bug Bounty chính thức được đưa vào hoạt động tại địa chỉ https://bugbounty.vn. Sự ra đời của Vietnam Bug Bounty được xem là một bước tiến lớn trong nỗ lực xây dựng cộng đồng bảo mật Việt Nam. Đây là một nền tảng kết nối giữa các chuyên gia, hacker mũ trắng trong lĩnh vực bảo mật an toàn thông tin với các doanh nghiệp, tổ chức có nhu cầu tìm kiếm lỗ hổng bảo mật tiềm tàng trong hệ thống vận hành của đơn vị.

Doanh nghiệp thông qua Trung tâm Giám sát an toàn không gian mạng quốc gia sẽ đưa ra các chương trình tìm kiếm lỗ hổng cùng các mức tiền thưởng trên Vietnam Bug Bounty. Sau đó, các chuyên gia bảo mật tham gia rà soát hệ thống, tấn công thử nghiệm, khai thác lỗ hổng theo phạm vi và chính sách chủ quản hệ thống đưa ra. Nếu phát hiện được lỗ hổng, điểm yếu có giá trị, chuyên gia đó sẽ được đơn vị chủ quản trả thưởng xứng đáng theo chính sách công bố ban đầu.

Với mô hình hoạt động này, các hacker mũ trắng, chuyên gia bảo mật sẽ có sân chơi chuyên nghiệp, lành mạnh để liên tục thực hành, nâng cao trình độ cũng như có cơ hội tạo ra mức thu nhập ổn định. Còn đối với doanh nghiệp, họ cũng giảm được các chi phí dịch vụ, tối ưu phí vận hành và nhanh chóng nhận được thông báo để kịp thời đối phó, xử lý sự cố an toàn thông tin.

Hệ thống Vietnam Bug Bounty được xây dựng trên Microservices - một nền tảng hiện đại đang trở thành xu hướng trên thế giới và được ứng dụng tại nhiều tập đoàn công nghệ lớn như eBay, Amazon, Netflix.... Những nghiệp vụ trên hệ thống đều được tư vấn, hỗ trợ bởi đội ngũ chuyên gia đến từ Trung tâm Giám sát an toàn không gian mạng quốc gia và VSEC để việc tìm kiếm lỗ hổng được thực hiện liên tục, song song với quá trình phát triển phần mềm.

Link tham khảo: https://thanhnien.vn/cong-nghe/ra-mat-cong-dong-ket-noi-hacker-mu-trang-va-chuyen-gia-bao-mat-1124131.html

2. Bản cập nhật mới nhất của Microsoft vá 4 lỗi nghiêm trọng trong Windows RDP Client

Microsoft vừa phát hành bản cập nhật Patch Tuesday tháng 9/2019, vá tổng cộng 79 lỗ hổng , trong đó 17 lỗi được đánh giá nghiêm trọng, 61 lỗi quan trọng và 1 lỗi có mức độ nghiêm trọng vừa phải.

Có hai lỗ hổng được liệt kê "đã được biết đến công khai" tại thời điểm phát hành, một trong số đó là lỗi leo thang đặc quyền (CVE-2019-1235) trong Khung dịch vụ văn bản Windows (TSF), nhiều khả năng liên quan đến lỗ hổng 20 năm tuổi đã được một nhà nghiên cứu của Google tiết lộ vào tháng trước.

Hai lỗ hổng khác đã bị tin tặc khai thác trong thực tế, cả hai đều là lỗ hổng leo thang đặc quyền - một nằm trong hệ điều hành Windows và một nằm trong Trình điều khiển hệ thống tệp nhật ký chung của Windows (Windows Common Log File System Driver).

Bên cạnh đó là bản vá cho bốn lỗ hổng RCE nghiêm trọng trong ứng dụng Remote Desktop Client được tích hợp trong Windows, có thể cho phép máy chủ RDP độc hại xâm nhập máy khách.

Các lỗ hổng này đều nằm ở phía máy khách, kẻ tấn công phải lừa nạn nhân kết nối với máy chủ RDP độc hại thông qua tấn công social engineering, DNS poisoning hoặc Man in the Middle (MITM).

Bản cập nhật cũng giải quyết lỗ hổng thực thi mã từ xa (CVE-2019-1280) trong cách hệ điều hành Windows xử lý các tệp shortcut .LNK, cho phép kẻ tấn công xâm nhập các hệ thống mục tiêu.

Bản cập nhật cũng vá 12 lỗ hổng nghiêm trọng khác, tất cả đều dẫn đến các cuộc tấn công thực thi mã từ xa và nằm trong các sản phẩm khác nhau của Microsoft gồm Chakra Scripting Engine, VBScript, SharePoint server, Scripting Engine, Azure DevOps và Team Foundation Server .

Một số lỗ hổng được xếp hạng quan trọng cũng dẫn đến các cuộc tấn công thực thi mã từ xa, trong khi các lỗ hổng khác cho phép nâng cao đặc quyền, tiết lộ thông tin, tấn công XSS, vượt qua tính năng bảo mật và tấn công từ chối dịch vụ.

Bên cạnh đó, nếu bạn có cài đặt Yammer, mạng xã hội doanh nghiệp của Microsoft trên điện thoại Android của mình, bạn nên cập nhật từ Google Play Store để vá lỗ hổng.

Người dùng và quản trị viên hệ thống được khuyến cáo cài đặt các bản vá Windows mới nhất từ Microsoft càng sớm càng tốt để ngăn chặn tội phạm mạng và tin tặc kiểm soát máy tính của họ.

Để cài đặt các bản cập nhật mới nhất, bạn có thể vào Settings → Update & Security → Windows Update → Check for updates trên máy tính của bạn hoặc bạn có thể cài đặt các bản cập nhật theo cách thủ công.

Adobe cũng vừa tung ra bản cập nhật khắc phục hai lỗ hổng thực thi mã từ xa trong Adobe Flash Player và một lỗi chiếm quyền điều khiển DLL trong Adobe Application Manager (AAM). Người dùng phần mềm Adobe bị ảnh hưởng nên cập nhật các gói phần mềm lên phiên bản mới nhất càng sớm càng tốt.

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://whitehat.vn/threads/ban-cap-nhat-moi-nhat-cua-microsoft-va-4-loi-nghiem-trong-trong-windows-rdp-client.12692/

3. Ứng dụng Android độc hại xuất hiện hai lần trên Google Play

Ứng dụng độc hại có tên là Radio Balouch, được phát hiện chứa mã độc Android/Spy.Agent.AOX. Giao diện ứng dụng được mô phỏng như một ứng dụng nghe radio bằng Internet, chuyên phát nhạc của người Baloch định cư tại Iran, Afghanistan và Pakistan.

Tuy nhiên, nhà nghiên cứu Lukas Stefanko thuộc công ty ESET đã chỉ ra rằng, ứng dụng này được tạo ra để theo dõi những người đã tải ứng dụng. Trong khi người

dùng sử dụng ứng dụng, mã độc gián điệp tiến hành các hoạt động đánh cắp thông tin danh bạ và thu thập các tệp được lưu trữ trên thiết bị.

Ngay sau khi được ESET đã báo cáo, Google đã xóa ứng dụng độc hại Radio Balouch trong vòng 24 giờ, nhưng 10 ngày sau ứng dụng này được nhà phát triển ban đầu đăng lại trên cửa hàng ứng dụng Google Play.

Ông Stefanko cho biết, công ty cũng đã phát hiện và báo cáo trường hợp thứ hai của mã độc và sau đó nó cũng được gỡ bỏ nhanh chóng. Tuy nhiên, việc Google cho phép cùng một nhà phát triển đăng lại một mã độc đã bị phát hiện lên cửa hàng ứng dụng nhiều lần là điều đáng lo ngại.

Ứng dụng Radio Balouch xuất hiện lần đầu tiên trên Google Play vào ngày 2/7, lần thứ hai vào ngày 13/7 và đều nhanh chóng bị gỡ bỏ. Mỗi lần đăng trên Google Play, ứng dụng đã được hơn 100 người cài đặt.

Radio Balouch có thể là ứng dụng chứa mã độc gián điệp Android nguồn mở đầu tiên xuất hiện trên Google Play, nhưng không có gì đảm bảo đây là ứng dụng cuối cùng. Vì ứng dụng độc hại vẫn có thể trở lại cửa hàng ứng dụng Google Play một cách dễ dàng sau khi bị xóa, nên Google cần đưa ra các biện pháp bảo mật nghiêm ngặt hơn.

Nếu Google không nâng cao khả năng bảo vệ an toàn cho người dùng, thì một bản sao mới của Radio Balouch hoặc bất kỳ mã độc dựa trên công cụ gián điệp AhMyth có thể sẽ sớm xuất hiện trên Google Play. Radio Balouch đã biến mất khỏi Google Play, nhưng nó vẫn có thể ở trên các cửa hàng ứng dụng khác.

ESET cho biết, ứng dụng Radio Balouch đã được quảng cáo trên một trang web chuyên dụng, Instagram và YouTube. Công ty đã báo cáo sự nguy hiểm của chiến dịch tấn công này cho các nhà cung cấp dịch vụ, nhưng không nhận được bất kỳ phản hồi nào.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng Android cần lưu ý - không cài ứng dụng lạ và đọc kỹ các chính sách của ứng dụng mới khi cài đặt để đảm bảo an toàn thông tin.

Link tham khảo: http://www.antoanthongtin.vn/Detail.aspx?CatID=c74b5c11-1141-471b-95c8-a05fe6e7d3a6&NewsID=fd78965a-cb0a-462f-a0a8-9f2b8ce504c4

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	Exim	CVE-2019-15846	Lỗ hổng nghiêm trọng trong Exim phiên bản 4.92.2 trở về trước cho phép đối tượng tấn công thực thi mã lệnh với quyền người dùng cao nhất trên hệ thống. Có 33.187 máy chủ của Việt Nam sử dụng Exim đang public trên Internet có khả năng bị khai thác.	Đã có thông tin xác nhận và bản vá.
2	Freebsd	CVE-2019-5608 CVE-2019-5609 CVE-2019-5610 ...	Nhóm 05 lỗ hổng trên hệ điều hành Freebsd cho phép đối tượng tấn công khai thác lỗi tràn bộ đệm, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
3	Android	CVE-2019-9245 CVE-2019-9248 CVE-2019-9442 ...	Nhóm 46 lỗ hổng trên hệ điều hành Android cho phép đối tượng tấn công thực hiện thu thập thông tin, tấn công leo thang,	Đã có thông tin xác nhận và bản vá
4	Cisco	CVE-2019-1968 CVE-2019-1969 CVE-2019-1976	Nhóm 12 lỗ hổng trên một số sản phẩm của Cisco (Cisco NX-OS Software, Unified Contact Center Express,) cho phép đối tượng tấn công khai thác lỗi SSRF, tấn công từ chối dịch vụ, thu thập thông tin trái phép, một số lỗ hổng cho phép chèn và thực thi mã lệnh.	Đã có thông tin xác nhận và bản vá
5	D-link	CVE-2019-10891 CVE-2019-10892 ...	Nhóm 02 lỗ hổng trên thiết bị D-Link DIR-806 cho phép đối tượng tấn công chèn và thực thi mã lệnh qua thành phần "SOAPAction: http://purenetworks.com/HNAP1/GetDeviceSettings/"	Chưa 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	mtmdj33s0.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.