BẢN TIN NỘI BỘ

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

1. Báo động nền tảng website WordPress bị hacker tấn công lừa đảo

Cuối tháng 3/2019, thông tin plugin (thành phần mở rộng được cài đặt thêm) có tên "Yuzo Related Posts" được cài trên hơn 60.000 website đã bị xóa bỏ khỏi thư viện plugin của Wordpress.org sau khi chứa lỗ hổng không có bản vá và được tiết lộ bởi một nhà nghiên cứu về bảo mật đã gây xôn xao trong cộng đồng công nghệ.

Về bản chất, lỗ hổng này cho phép thực hiện tấn công dạng Stored-XSS và hiện đang bị lợi dụng để tấn công các website sử dụng nền tảng WordPress có cài đặt plugin.

Với việc sử dụng lỗ hổng này, các cuộc tấn công có thể vượt qua cơ chế bảo vệ của Wordfence ("tường lửa" của WordPress) khiến một kẻ tấn công không cần quyền xác thực cũng có thể chèn các nội dung độc hại, ví dụ như một đoạn mã Javascript vào trong cấu hình của plugin.

Lỗ hổng này có thể lợi dụng để tấn công thay đổi giao diện để lừa đảo người dùng.

11 ngày sau khi lỗ hổng bị phát hiện, các hacker đã tuyên bố bắt đầu khai thác các trang web có cài đặt "Yuzo Related Posts".

Khi người dùng truy cập website đã bị khai thác, đoạn mã javascript từ máy chủ hellofromhony.com sẽ chuyển hướng họ tới các website lừa đảo hoặc chứa mã độc.

Phân tích của SecurityBox cho thấy hình thức tấn công này có nhiều điểm tương đồng với tấn công dựa vào 2 lỗ hổng được phát hiện trước đó có tên là Social Warfare và Easy WP SMTP (mã độc cùng được lưu trữ trên máy chủ hellofromhony.org có địa chỉ IP 176.123.9[.]53).

Cả 3 cuộc tấn công đều sử dụng lỗ hổng Stored-XSS và chuyển hướng người dùng tới các website độc hại để tiến hành lừa đảo.

Do đó, kỹ thuật tấn công và quy trình khai thác cho cả 3 lỗ hổng này khả năng rất lớn đều do một tin tặc gây ra.

Trước thực trạng đáng lo ngại trên, phía SecurityBox khuyến cáo chủ sở hữu các trang web cài đặt plugin Yuzo Related Posts phải gỡ bỏ ngay lập tức cho đến khi có bản vá sửa lỗi chính thức.

Với các khách hàng sử dụng bản miễn phí, do thời gian chờ đợi bản cập nhật là 30 ngày nên việc gỡ bỏ ra khỏi website sẽ tránh được rủi ro bị tấn công.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng và quản trị viên cần gỡ bỏ ngay lập tức plugin "Yuzo Related Posts" trên trình duyệt để đảm bảo an toàn thông tin.

Link tham khảo: https://ictnews.vn/cntt/bao-mat/bao-dong-nen-tang-website-wordpress-bi-hacker-tan-cong-lua-dao-181211.ict

2. Lỗi bảo mật trong giao thức WPA3 giúp hacker lấy mật khẩu Wi-Fi

"WPA" là viết tắt của Wi-Fi Protected Access, một giao thức bảo mật cho mạng Wi-Fi. Giao thức Wi-Fi Protected Access III (WPA3) đã được đưa ra trong nỗ lực giải quyết các thiếu sót kỹ thuật của giao thức WPA2, từ lâu đã được coi là không an toàn và dễ bị KRACK (Tấn công cài đặt lại khóa).

WPA3 được giới thiệu sẽ mang lại sự bảo vệ mạnh mẽ ngay cả khi người dùng chọn mật khẩu ngắn và không phức tạp. Nói cách khác, ngay cả khi bạn đang sử dụng một mật khẩu yếu, tiêu chuẩn WPA3 sẽ bảo vệ chống lại các cuộc tấn công brute-force. Đây là kiểu tấn công mà một máy khách cố gắng đoán mật khẩu, hành động này lặp đi lặp lại cho đến khi nó tìm được mật khẩu chính xác. Mathy Vanhoef, nhà nghiên cứu bảo mật đã phát hiện ra KRACK, tỏ ra rất thích về những cải tiến bảo mật trong WPA3.

Tuy nhiên, có vẻ như công nghệ nào cũng có nhiều lỗ hổng, và WPA3 cũng vậy. Mặc dù WPA3 dựa vào một giao thức kết nối-giao tiếp an toàn hơn, được gọi là Dragonfly nhằm bảo vệ các mạng Wi-Fi chống lại các cuộc tấn công ngoại tuyến.

Các nhà nghiên cứu bảo mật Mathy Vanhoef và Eyal Ronen đã tìm thấy điểm yếu trong việc triển khai sớm WPA3-Personal, cho phép kẻ tấn công khôi phục mật khẩu Wi-Fi dễ dàng bằng cách sử dụng kỹ thuật liên quan đến abusing timing (mã lỗi CVE-2019-9494) hoặc lấy được cache-based side-channel (mã lỗi CVE-2019-9494).

Cụ thể, những kẻ tấn công có thể đọc thông tin WPA3 được cho là mã hóa an toàn. Điều này có thể bị lạm dụng để đánh cắp thông tin nhạy cảm như số thẻ tín dụng, mật khẩu, tin nhắn trò chuyện, email,...

"Để tấn công phân vùng lưu trữ mật khẩu, chúng tôi cần ghi lại một số lần liên kết với các địa chỉ MAC khác nhau. Chúng tôi có thể kết nối với các địa chỉ MAC khác nhau bằng cách nhắm mục tiêu nhiều khách hàng trong cùng một mạng (ví dụ: thuyết phục nhiều người dùng tải xuống cùng một ứng dụng độc hại). Hoặc trường hợp chỉ có thể tấn công một thiết bị, chúng tôi có thể thiết lập các trạm lừa đảo có cùng SSID nhưng địa chỉ MAC giả mạo." - Hai nhà nghiên cứu cho biết.

Bên cạnh đó, nghiên cứu cũng ghi nhận một cuộc tấn công từ chối dịch vụ (DoS) có thể được khởi chạy bằng cách khởi động một số lượng lớn các kết nối với Access Point hỗ trợ WPA3, bỏ qua cơ chế chống tắc nghẽn của SAE được cho là để ngăn chặn các cuộc tấn công DoS.

Hiện tại nghiên cứu này đã được báo cáo cho WiFi Alliance, tổ chức phi lợi nhuận chứng nhận các tiêu chuẩn WiFi và các sản phẩm Wi-Fi phù hợp. Họ đã thừa nhận các vấn đề và đang làm việc với các nhà cung cấp để vá các thiết bị được chứng nhận WPA3 hiện có.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần cập nhật bản vá mới nhất của các thiết bị accesspoint hỗ trợ WPA3 từ nhà sản xuất để đảm bảo an toàn thông tin.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/loi-bao-mat-trong-giao-thuc-wpa3-giup-hacker-lay-mat-khau-wi-fi-521488.html

3. Ngân hàng phải hướng dẫn khách hàng giao dịch trực tuyến an toàn

Ngân hàng Nhà nước Việt Nam vừa ban hành văn bản về việc đẩy mạnh thanh toán điện tử trong lĩnh vực dịch vụ công.

Theo đó, tiếp tục chú trọng nghiên cứu và triển khai áp dụng các giải pháp công nghệ tiên tiến để cải tiến quy trình nghiệp vụ, tối ưu hóa quy trình xử lý nhằm cung ứng đa dạng các sản phẩm, dịch vụ thanh toán chất lượng, phù hợp với nhu cầu của các tổ chức, cá nhân với chi phí hợp lý để thanh toán thuận tiện, nhanh chóng, an toàn đối với các khoản phí, lệ phí, thanh toán hóa đơn điện, nước, học phí, viện phí...

Nghiên cứu giải pháp về mô hình kết nối phù hợp, hiệu quả giữa các ngân hàng, tổ chức cung ứng dịch vụ trung gian thanh toán với Cổng dịch vụ công quốc gia, Hệ thống một cửa điện tử của các Bộ, ngành, địa phương, các cơ quan, đơn vị liên quan nhằm đơn giản hóa thủ tục và tạo điều kiện thanh toán điện tử đối với các khoản phí, lệ phí, thanh toán hóa đơn điện, nước, học phí, viện phí... một cách nhanh chóng, an toàn.

Hướng dẫn và phổ biến đầy đủ, kịp thời cho khách hàng biết về quy trình thủ tục, thao tác thực hiện và các biện pháp đảm bảo an toàn khi thực hiện giao dịch thanh toán điện tử nói chung cũng như thanh toán trực tuyến đối với các khoản phí, lệ phí, thanh toán hóa đơn điện, nước, học phí, viện phí...

Thiết lập bộ phận hỗ trợ tiếp nhận và xử lý kịp thời các vướng mắc, tra soát, khiếu nại phát sinh nếu có trong qúa trình thực hiện.

Bên cạnh đó, chỉ đạo các chi nhánh, đơn vị trực thuộc thường xuyên kiểm tra các điều kiện về hạ tầng kỹ thuật, chương trình phần mềm phục vụ thanh toán điện tử, đảm bảo thực hiện các lệnh thanh toán nộp phí, lệ phí, thanh toán hóa đơn điện, nước, học phí, viện phí,... của khách hàng một cách chính xác, kịp thời, thông suốt và an toàn theo đúng quy định.

Trường hợp có phát sinh sai sót hoặc tra soát, khiếu nại phải kiểm tra, xác định nguyên nhân và phối hợp chặt chẽ với các đơn vị liên quan để phản hồi, giải thích rõ lý do cho khách hàng biết..

Link tham khảo: https://ictnews.vn/cntt/bao-mat/ngan-hang-phai-huong-dan-khach-hang-giao-dich-truc-tuyen-an-toan-181109.ict

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	IBM	CVE-2018-1936 CVE-2019-4014 CVE-2018-1640 CVE-2018-1906 CVE-2018-1917 CVE-2018-1618 CVE-2018-1622 ...	Nhóm 18 lỗ hổng trên một số sản phẩm, ứng dụng của IBM (API Connect, DB2 Linux/ Windows, Rational Engineering Lifecycle Manage, IBM SDK, WebSphere Application Server...) cho phép đối tượng tấn công thực hiện thu thập thông tin, khai thác các lỗi tràn bộ đệm để chèn và thực thi mã lệnh, tấn công leo thang.	Đã có thông tin xác nhận và bản vá
2	Apple	CVE-2018-4126 CVE-2018-4327 CVE-2018-4268 CVE-2018-4291 …	Nhóm 185 lỗ hổng trong một số sản phẩm của Apple. Một ứng dụng độc hại truy cập tài khoản, tự động mở khóa AppleIDs của người dùng cục bộ và thực thi mã tùy ý với đặc quyền của hệ thống. Sự cố này ảnh hưởng đến các phiên bản trước IOS 12, macOS Mojave 10.14, tvOS 12, watchOS 5, Itunes 12.9 cho Windows, iCloud.	Đã có thông tin xác nhận và bản vá
3	Jenkins	CVE-2019-10298 CVE-2019-1003096 CVE-2019-1003098 CVE-2019-10294 CVE-2019-10289 ...	Nhóm 72 lỗ hổng trên phần mềm Jenkins (phần mềm sử dụng trong phát triển phần mềm) cho phép đối tượng tấn công thu thập thông tin xác thực lưu trữ trong cấu hình của Plugin, một số lỗ hổng cho phép chèn và thực thi mã lệnh.	Chưa có thông tin xác nhận và bản vá.
4	Cisco	CVE-2019-1827 CVE-2019-1828 …	Nhóm 02 lỗ hổng trên một số sản phẩm của Cisco (các dòng switch Nexus, NX-OS, FXOS Software,) cho phép truy cập và thông tin nhạy cảm lưu trữ	Đã có thông tin xác nhận và bản vá.

			trên hệ thống, chèn và thực thi mã lệnh để chiếm quyền kiểm soát thiết bị.	

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

STT	**Tên miền/IP**
1	plpanaifheaighai.com
2	n.hmiblgoja.ru
3	ajkeahkcueafuiaeuf.ru
4	iuefgauiaiduihgs.com
5	mokoaehaeihgiaheih.ru
6	43trfdsds.com
7	bszotsjovih.com
8	https://kisscherrygirls.com/xefyzznumsa
9	mel.cloudcontentsmak.com
10	strikotunrev.top

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.