BẢN TIN NỘI BỘ

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

1. WEB JOOMLA và WORDPRESS bị tấn công và phát tán mã độc

Trong một vài tuần vừa qua, các nhà nghiên cứu đã phát hiện một loạt các mối nguy hại được ẩn giấu trong đường dẫn ẩn trong giao thức HTTPS, trong đó có mã độc tống tiền Shade – tên khác là Troldesh – phần mềm độc hại phổ biến nhất được triển khai theo cách này.

"Các email spam thường chứa liên kết tới một trang chuyển hướng HTML đặt trên trang web đã bị tấn công, nếu người dùng ấn vào đó sẽ tải về một tập tin nén zip độc hại. Người dùng cần phải mở tập tin JavaScript bên trong file ZIP đó và file JavaScript này sẽ tải phần mềm độc hại về từ trang web đã bị tấn công và kích hoạt nó," Deepen Desai, Phó Chủ tịch phụ trách nghiên cứu và thực thi bảo mật của Zscaler trả lời phỏng vấn của trang tin ZDNet.

Đã có hơn 500 trang web bị tấn công và hàng nghìn lượt tải đã được thực hiện nhằm phát tán các mã độc tống tiền, liên kết lừa đảo (phishing) và nhiều loại nội dung nguy hại khác.

Mặt khác, các trang lừa đảo dạng phishing được lưu trữ trong các đường dẫn ẩn đã được chứng thực mã hoá SSL, điều đó khiến những người dùng không chú ý kĩ có thể bị lừa cung cấp tên đăng nhập và mật khẩu của mình cho những kẻ tấn công.

Các trang web bị tấn công sử dụng WordPress các phiên bản từ 4.8.9 đến 5.1.1 và dường như đã sử dụng các giao diện cũ không được cập nhật bảo mật, hoặc các phần mềm lỗi thời được cài đặt trên máy chủ. Đây có thể là những nguyên nhân mà các nhà nghiên cứu cho là lý do khiến các website này trở thành mục tiêu của kẻ tấn công.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần cập nhật những phiên bản mới nhất của các trình duyệt cũng như Joomla và Wordpress (nếu đang sử dụng) để đảm bảo an toàn thông tin.

Link tham khảo: https://securitybox.vn/7642/web-joomla-va-wordpress-bi-tan-cong-va-phat-tan-ma-doc/

2. Apache tồn tại lỗ hổng đe dọa an ninh các máy chủ web

Người dùng vừa được cảnh bảo về một lỗ hổng quan trọng trong phần mềm Apache HTTP Server. Cảnh báo được Mark J Cox, một trong những thành viên sáng lập của Quỹ phần mềm Apache và dự án OpenSSL đưa ra.

Máy chủ web Apache là một trong những máy chủ web nguồn mở phổ biến nhất, được sử dụng rộng rãi trên thế giới.

Lỗ hổng này, CVE-2019-0211, đã được các nhà phát triển Apache vá trong phiên bản mới nhất 2.4.39.

Lỗ hổng ảnh hưởng đến Apache HTTP Server phiên bản 2.4.17 đến 2.4.38 và có thể cho phép bất kỳ người dùng ít đặc quyền thực thi mã tùy ý với quyền root trên máy chủ mục tiêu.

Theo Cox, lỗ hổng ảnh hưởng nhiều đến các dịch vụ lưu trữ web chia sẻ (shared hosting), cho phép kẻ xấu với khả năng thực thi các tập lệnh PHP hoặc CGI trên trang web có được quyền truy cập root trên máy chủ, cuối cùng truy cập được dữ liệu của website khác được lưu trữ trên cùng máy chủ.

Bên cạnh đó, phiên bản Apache httpd 2.4.39 mới nhất cũng vá hai vấn đề quan trọng và ba vấn đề có mức độ nghiêm trọng thấp. Hai lỗ hổng quan trọng, CVE-2019-0217 và CVE-2019-0215, đều cho phép vượt qua các hạn chế kiểm soát truy cập.

Các dịch vụ lưu trữ web, các tổ chức quản lý máy chủ riêng và quản trị viên trang web được khuyến khích nâng cấp các phiên bản Apache HTTP lên các phiên bản mới nhất càng sớm càng tốt.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng và quản trị viên cần cập nhật ngay phiên bản mới nhất của Apache để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/apache-ton-tai-lo-hong-de-doa-an-ninh-cac-may-chu-web.12125/

3. Ứng dụng diệt virus trên điện thoại Xiaomi bị hacker 'biến' thành malware

Một ứng dụng an ninh cài đặt sẵn trên khoảng 150 triệu thiết bị Xiaomi có thể bị hacker từ xa khai thác để chiếm quyền điều khiển điện thoại.

Theo công ty bảo mật CheckPoint, ứng dụng tồn tại lỗ hổng trên được Xiaomi phát triển và có tên Guard Carrier. Đây là một ứng dụng tích hợp 3 chương trình diệt virus khác nhau cho phép người dùng lựa chọn là Avast, AVL và Tencent.

Vì sử dụng bộ phát triển phần mềm (SDK) nên Guard Provider có thể cung cấp nhiều chương trình của bên thứ 3 trong một ứng dụng. Tuy nhiên, theo các nhà nghiên cứu, đây không phải là giải pháp tối ưu vì dữ liệu của một SDK không thể tách biệt, và nếu 1 SDK tồn tại lỗ hổng thì có thể khiến các SDK còn lại đứng trước nguy cơ bị tấn công.

Cũng theo hãng bảo mật Checkpoint, các lỗ hổng nhỏ và độc lập trong một SDK có thể trở nên nghiêm trọng hơn do nhiều SDK được triển khai trong cùng một ứng dụng.

Ứng dụng Guard Carrier tải các bản cập nhật diệt virus thông qua kết nối HTTP không an toàn, cho phép hacker thực hiện tấn công man-in-the-middle để can thiệp vào kết nối mạng trên thiết bị nạn nhân và chèn malware vào các bản cập nhật.

Theo Checkpoint, sau khi kết nối với cùng một mạng Wi-Fi của nạn nhân –ví dụ tại những nơi công cộng như nhà hàng, quán cà phê hoặc trung tâm thương mại - kẻ tấn công có thể truy cập hình ảnh, video và dữ liệu nhạy cảm khác của chủ sở hữu điện thoại, hoặc chèn phần mềm độc hại vào máy nạn nhân.

Tuy nhiên, kịch bản tấn công trên thực tế không hề đơn giản.

Các nhà nghiên cứu của Checkpoint đã thực thi mã từ xa thành công trên thiết bị Xiaomi sau khi khai thác bốn lỗ hổng riêng biệt trong hai SDK khác nhau có sẵn trong ứng dụng.

Check Point đã báo cáo lỗ hổng tới Xiaomi và được hãng xác nhận đã khắc phục lỗ hổng trong phiên bản mới nhất của ứng dụng Guard Carrier.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng smartphone Xiaomi cần cập nhật phần mềm bảo mật trên điện thoại trong thời gian sớm nhất để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/ung-dung-diet-virus-tren-dien-thoai-xiaomi-bi-hacker-%E2%80%98bien%E2%80%99-thanh-malware.12133/

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-2019-4052 CVE-2019-4035 CVE-2019-4046 ...	Nhóm 03 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	Apache	CVE-2019-0204 CVE-2019-0222 CVE-2019-0212 CVE-2019-0225 CVE-2019-0224 CVE-2019-7608 CVE-2019-7609 CVE-2019-7610 …	Nhóm 08 lỗ hổng trong một số sản phẩm của Apache (JMeter, Solr, Qpid Broker-J, Apache Traffic Server) cho phép đối tượng tấn công thực hiện thu thập thông tin, chèn và thực thi mã lệnh trong phạm vi của ứng dụng.	Đã có thông tin xác nhận và bản vá
3	Jenkins	CVE-2019-1003048 CVE-2019-1003047 CVE-2019-1003046 CVE-2019-1003045 CVE-2019-1003044 ...	Nhóm 9 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, thực thi mã lệnh.	Đã có thông tin xác nhận và bản vá.
4	Cisco	CVE-2019-1749 CVE-2019-1750 CVE-2019-1758 CVE-2019-1757 CVE-2019-1746 …	Nhóm 25 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 trên hệ thống, chèn và thực thi mã lệnh để chiếm quyền kiểm soát.	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	localhost.localdomain
2	n.hmiblgoja.ru

3	ajkeahkcueafuiaeuf.ru
4	mokoaehaeihgiaheih.ru
5	43trfdsds.com
6	iuefgauiaiduihgs.com
7	bszotsjovih.com
8	strikotunrev.top
9	mel.cloudcontentsmak.com
10	d3s1.me

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.