BẢN TIN NỘI BỘ

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

1. Microsoft Excel dính lỗ hổng bảo mật liên quan 120 triệu người dùng

Theo Fortune, lỗ hổng bảo mật do một nhóm chuyên gia tại Mimecast phát hiện ra nằm trong Power Query - công cụ cho phép người dùng tích hợp bảng tính với cơ sở dữ liệu, tài liệu văn bản và trang web bên ngoài. Lỗ hổng này có thể cho phép kẻ tấn công chiếm lấy hệ thống của người dùng và chạy các phần mềm độc hại từ xa. Nếu bị khai thác, lỗ hổng này cũng có thể khởi động các cuộc tấn công tinh vi, khó phát hiện hơn.

Lỗ hổng dựa trên một phương pháp tấn công gọi là trao đổi dữ liệu động (Dynamic Data Exchange - DDE). Tấn công bằng phương pháp này khá phổ biến, nhưng đáng chú ý vì nó mang đến cho những kẻ xâm nhập đặc quyền quản trị.

Công ty cho biết "khi sử dụng Power Query, những kẻ tấn công có thể nhúng nội dung độc hại vào một nguồn dữ liệu riêng biệt, sau đó nạp nội dung vào bảng tính khi nó được mở. Mã độc có thể được sử dụng để thực thi phần mềm độc hại gây tổn hại đến máy của người dùng".

Mimecast nói thêm "vì Power Query là một công cụ mạnh mẽ trong Microsoft Excel, mối đe dọa tiềm tàng cho việc lạm dụng tính năng này là rất lớn. Sử dụng điểm yếu tiềm ẩn trong Power Query, kẻ tấn công có khả năng nhúng bất kỳ nội dung độc hại được thiết kế sẽ không lưu bên trong tài liệu nhưng được tải xuống từ web khi tài liệu được mở ra".

Microsoft hiện vẫn chưa đưa ra một bản sửa lỗi cho lỗ hổng tại thời điểm hiện tại, nhưng đã phát hành một tài liệu tư vấn cho người dùng, cung cấp một cách giải quyết để tăng cường bảo mật.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần cảnh giác khi sử dụng tài liệu Excel có kết nối tới các đường link lạ, luôn đề cao cảnh giác với các tin nhắn không rõ nguồn gốc, tránh click vào đường link lạ nhận được từ mail hoặc các ứng dụng chat để đảm bảo an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/microsoft-excel-dinh-lo-hong-bao-mat-lien-quan-120-trieu-nguoi-dung-1098071.html

2. Lừa đảo trúng thưởng từ Google

Chiến dịch lừa đảo này đã gửi đi một loạt email spam thông báo cho các nạn nhân rằng Google sẽ trao cho họ 2,5 triệu đô la tiền thưởng như một phần của chương trình tri ân những khách hàng trung thành với các dịch vụ của Google trong nhiều năm.

Trò lừa đảo này xuất hiện dưới dạng một email với dòng tiêu đề "Powered by Google" như một sự khẳng định về mức độ uy tín, nói rằng "Bạn đã được chọn là một trong những người chiến thắng giải thưởng người dùng trung thành đối với các dịch vụ của Google" (You have been selected a winner for using Google services).

Để tăng thêm tính hợp pháp, kẻ gian bổ sung thêm dòng quảng cáo rằng email này đang được gửi cho bạn bởi một Giám đốc quản lý bộ phận, thay mặt cho CEO Google, Larry Page.

Đi cùng với email lừa đảo này là một tệp đính kèm có tên "Official Winning Letter by Google and mastercard visa 2019.pdf". Tệp đính kèm này, như được hiển thị ở ảnh chụp màn hình bên dưới, nói rằng bạn đã giành được giải thưởng Google Visa/MasterCard (GVMC) với tổng giá trị lên tới 2.500.000 USD!

Ở bước tiếp theo kẻ gian bắt đầu "vào vấn đề chính" khi yêu cầu nạn nhân phải điền đầy đủ và chính xác thông tin được yêu cầu và gửi lại cho chúng để nhận giải thưởng. Còn kết cục thì như chúng ta đã biết, sẽ chẳng có một đồng nào được chuyển lại, trong khi những thông tin cá nhân cực kỳ quan trọng của bạn như thông tin tài khoản ngân hàng, thẻ tín dụng, số điện thoại và thậm chí là cả tài khoản, mật khẩu đã rơi vào tay kẻ gian.

Đặc biệt có một chi tiết mà chúng ta thường bắt gặp trên hầu hết các email lừa đảo nói chung, đó là lời cảnh báo phải giữ bí mật hoàn toàn đối với thông tin mà bạn nhận được. Như trong trường hợp này, kẻ gian yêu cầu nạn nhân "giữ kín thông tin giải thưởng cho mục đích bảo mật và tránh các hành vi lạm dụng khác". Tuy nhiên mục đích thực sự của những yêu cầu dạng này đơn giản chỉ là không để nạn nhân tiết lộ thông tin cho những người tỉnh táo hơn, dẫn đến hành vi lừa đảo bị bại lộ. Do đó, đây cũng là một đặc điểm thường gặp trong mọi hành vi lừa đảo nói chung mà bạn cần lưu ý.

Ở phần cuối của tệp đính kèm, kẻ lừa đảo yêu cầu bạn "Vui lòng cân nhắc kỹ tác hại liên quan đến môi trường trước khi quyết định in email này!" (Please consider the environment before printing!). Thực ra chúng chẳng quan tâm đến môi trường lắm đâu, mà mục đích sau cùng vẫn là ngăn việc nạn nhân để lộ email này cho những người "tỉnh táo hơn", khiến hành vi lừa đảo của chúng bị phát giác.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng tuyệt đối không mở tệp đính kèm trong email, không trả lời email cũng như cung cấp bất cứ thông tin nào theo yêu cầu của kẻ lừa đảo và báo ngay cho đầu mối phụ trách ATTT của đơn vị để xử lý.

Link tham khảo: https://quantrimang.com/lua-dao-trung-thuong-164779

3. Vá các lỗ hổng nghiêm trọng trong các sản phẩm Cisco

Theo Cisco, trung tâm kiến trúc mạng kỹ thuật số (DNA) bị ảnh hưởng bởi lỗ hổng nghiêm trọng cho phép kẻ tấn công vượt qua xác thực và truy cập vào các dịch vụ nội bộ quan trọng.

Cùng với đó, giải pháp giao diện dòng lệnh SD-WAN bị ảnh hưởng bởi một lỗ hổng nghiêm trọng có thể bị kẻ tấn công khai thác nhằm leo thang đặc quyền, từ đó root và thay đổi cấu hình hệ thống.

SD-WAN còn bị ảnh hưởng bởi lỗ hổng có mức độ nghiêm trọng cao cho phép leo thang đặc quyền thông qua giao diện người dùng web vManage, cùng một vấn đề

an ninh khác có thể bị hacker khai thác để xác thực từ xa và thực thi các lệnh với đặc quyền root.

Một lỗ hổng DoS có mức độ nghiêm trọng cũng 'cao' được tìm thấy trên hệ điều hành StarOS và một số bộ định tuyến RV, có thể bị thác từ xa mà không cần xác thực.

Các lỗ hổng khác được vá trong lần này bao gồm cross-site request forgery (CSRF) trong phần mềm Prime Service Catalog và Command injection trong Meeting Server và một số phần mềm TelePresence.

Bên cạnh đó, Cisco cũng đã khắc phục hàng tá sự cố ở mức độ nghiêm trọng trung bình trong Wide Area Application Services (WAAS), bộ định tuyến RV, Prime Service Catalog…

Cisco cho biết, không có bằng chứng nào cho thấy những lỗ hổng này bị khai thác nhằm mục đích xấu. Nhiều lỗ hổng đã được phát hiện bởi chính Cisco trong quá trình kiểm tra nội bộ.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng và quản trị viên cần cập nhật các bản vá mới nhất của các sản phẩm nêu trên để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/va-cac-lo-hong-nghiem-trong-trong-cac-san-pham-cisco.12410/

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	Cisco	CVE-2019-1623 CVE-2019-1874 CVE-2019-1875 ...	Nhóm 25 lỗ hổng dựa trên một số sản phẩm của Cisco (Cisco Meeting Server IMC, Cisco Prime Service Catalog ..) cho phép kẻ tấn công chèn và thực thi mã lệnh với quyền cao Root, thực hiện tấn công từ chối dịch vụ, khai thác lỗ XSS, nhiều lỗ hổng cho phép vượt qua các cấu hình bảo mật để truy cập trái phép vào các vùng mạng.	Đã có thông tin xác nhận và bản vá
2	IBM	CVE-2019-4364 CVE-2019-4103 CVE-2019-4384 …..	Nhóm 14 lỗ hổng dựa trên một số sản phẩm của IBM (InfoSphere Information Server, IOC, ISIQ) cho phép kẻ tấn công nhúng các đoạn mã JavaScript để lấy thông tin xác thực.	Đã có thông tin xác nhận và bản vá
3	Stopzilla	CVE-2019-0175 CVE-2019-0181 CVE-2019-0164 CVE-2019-0177 ……..	Nhóm 09 lỗ hổng dựa trên STOPzilla AntiMalware cho phép thực hiện tấn công từ chối dịch vụ, khai thác lỗi tràn bộ đệm để ghi dữ liệu độc hịa lên một số thành phần điều khiển.	Đã có thông tin xác nhận và bản vá.
4	Google	CVE-2018-9561 CVE-2018-9563 CVE-2018-9564 CVE-2018-9564 ……	Nhóm 29 lỗ hổng hệ điều hành Android cho phép đối tượng tấn công thực hiện thu thập thông tin, chèn và thực thi mã lệnh trái phép từ xa, tấn công leo thang.	Đã có thông tin xác nhận và bản vá.
5	Whatsapp	CVE-2018-20655 CVE-2018-6350 CVE-2018-6349	Nhóm 03 lỗ hổng trên phần mềm Whatsapp cho phép đối tượng tấn công khai thác lỗi tràn bộ đệm để chèn và thực	Đã có thông tin xác nhận và bản vá.

			thi mã lệnh.	
6	Wordpress	CVE-2018-16613 CVE-2019-10270	Nhóm 02 lỗ hổng trên một số thành phần Wordpress (wpForo Forum, Ultimate Member) cho phép đối tượng tấn công thực hiện tấn công leo thang để chiếm quyền quản trị với quyền một người dùng thông thường, cho phép đặt lại mật khẩu của bất kỳ người dùng nào.	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	klocpdqc7n.ru
5	kodklq.info
6	xjpakmdcfuqe.com
7	646u38k6.ru
8	www.cityofangelsmagazine.com
9	34ksilb9u.ru
10	kodklq.info

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.