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

1. Hai lỗ hổng nghiêm trọng trong Adobe Acrobat, Reader đã được vá

Các bản cập nhật an ninh đầu tiên của Adobe cho năm 2019 đã giải quyết hai lỗ hổng nghiêm trọng trong các sản phẩm Acrobat và Reader, nhưng các quản trị viên không nên quá lo lắng về những lỗ hổng sẽ bị khai thác sớm.

Các phiên bản mới nhất của Acrobat DC, Acrobat Reader DC, Acrobat 2017 và Acrobat Reader DC 2017 cho Windows và macOS vá một lỗi Use-After-Free có thể dẫn đến việc thực thi mã tùy ý bằng quyền của người dùng hiện tại (CVE-2018-16011) và có thể vượt qua cơ chế an ninh dẫn đến lỗi leo thang đặc quyền (CVE-2018-19725).

Lỗ hổng đầu tiên được phát hiện bởi Sebastian Apelt và lỗi thứ hai được Abdul Aziz Hariri tìm ra. Cả hai lỗ hổng đều đã được báo cáo tới Adobe thông qua chương trình Zero Day Initiative của Trend Micro (trao thưởng cho việc phát hiện lỗ hổng zero-day).

Tuy cả hai lỗ hổng được coi là nghiêm trọng nhưng Adobe chỉ đánh giá chúng ở mức xếp hạng ưu tiên là 2, đồng nghĩa với việc khai thác chưa xảy ra trong thực tế và các quản trị viên nên cài đặt các bản vá trong vòng 30 ngày.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng và người quản trị cần cập nhật phiên bản mới nhất của phần mềm Adobe để tránh nguy cơ mất an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/hai-lo-hong-nghiem-trong-trong-adobe-acrobat-reader-da-duoc-va.11886/

2. Hacker chiếm quyền kiểm soát Chromecast để kêu gọi ủng hộ cho kênh YouTube của PewDiePie

Hai hacker vừa phối hợp với nhau để thể hiện tình yêu với Felix "PewDiePie" Kjellberg bằng cách tấn công các TV để khiến chúng hiển thị một tin nhắn khuyến khích mọi người đăng ký kênh YouTube của streamer người Thụy Điển. Vụ hack lợi dụng một thiết lập trên router có chức năng cho phép các thiết bị thông minh, như Chromecast và Google Home, có thể được xem công khai trên mạng Internet. Những kẻ tấn công đã nắm quyền kiểm soát được các thiết bị này và phát sóng các đoạn video trên một TV đã kết nối trước đó.

Vụ tấn công này - còn được gọi là CastHack - được tiến hành bởi hai hacker có biệt danh HackerGiraffe và j3ws3r. Hai thanh niên này đã lập nên một website để đếm số lượng TV đã bị tấn công nhằm hiển thị tin nhắn liên quan đến PewDiePie, và đến lúc này, con số đếm được đã lên đến hơn 3.000. Dù chưa rõ đây có phải là con số chính xác hay không (bởi website này đã reset nhiều lần), nhưng đã có kha khá người đăng lên Reddit rằng TV nhà họ đã bị tấn công và hiện ra một đoạn video.

Google cho biết họ đã nhận được tin báo từ nhiều người rằng có một đoạn video trái phép đang chạy trên TV của họ thông qua một thiết bị Chromecast, nhưng hóa ra, vấn đề này không xuất phát từ bản thân Chromecast mà là do các thiết lập trên

router. Cả HackerGiraffe và Google đều cho biết cách nhanh nhất để những người dùng bị ảnh hưởng khắc phục được lỗi là tắt thiết lập Universal Plug and Play (UPnP) trên router của họ đi.

Đây là lần thứ hai HackerGiraffe và j3ws3r phối hợp để ủng hộ PewDiePie thông qua những vụ hack khó chịu. Cả hai đều là những hacker đứng sau vụ hack hồi tháng 11 nhắm vào các máy in trên toàn thế giới, khiến chúng in ra nhiều trang giấy với nội dung khuyến khích mọi người đăng ký kênh YouTube của PewDiePie.

Những vụ hack này diễn ra trong bối cảnh Kjellberg đang trong một cuộc chiến với một kênh YouTube khác là T-Series, vốn có số lượt đăng ký xấp xỉ, và có khả năng vượt qua kênh của stream này.

HackerGiraffe cho biết những cuộc tấn công của họ thực ra có mục đích phơi bày những lỗ hổng bảo mật chứ không phải chỉ nhằm quảng cáo cho kênh YouTube PewDiePie. "Chúng tôi muốn giúp bạn, và cả các YouTuber yêu thích của chúng tôi nữa (chủ yếu là PewDiePie)" - đó là những gì được viết trên website của họ. "Chúng tôi chỉ đang cố bảo vệ bạn và thông báo cho bạn về lỗ hổng này trước khi có ai đó thực sự lợi dụng nó".

CastHack là cuộc tấn công nhằm nhắc nhở Google về các lỗ hổng bảo mật, HackerGiraffe nói. Những lỗ hổng này bao gồm việc "các dữ liệu nhạy cảm bị rò rỉ" và khả năng reset Chromecast từ xa. HackerGiraffe cho biết cuộc tấn công không hề thu thập thông tin từ các thiết bị bị ảnh hưởng; họ chỉ đổi tên chúng và buộc chúng phải chơi đoạn video trên YouTube của họ mà thôi.

Vào tháng 12 vừa qua, website của tờ Wall Street Journal cũng từng bị hack để quảng cáo cho kênh YouTube PewDiePie, nhưng HackerGiraffe cho biết họ vô can.

"Vụ tấn công Wall Street Journal là có ác ý và đi ngược lại với những tôn chỉ của chúng tôi", HackerGiraffe nói.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần cập nhật phiên bản mới nhất của Google Home cho thiết bị Chromecast và tắt tính năng UPnP trên thiết bị router để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/hacker-chiem-quyen-kiem-soat-chromecast-de-keu-goi-ung-ho-cho-kenh-youtube-cua-pewdiepie.11887/

3. Hacker sử dụng tấn công Phishing tự động để phá vỡ bảo mật 2 yếu tố

Cụ thể, nhóm này vào hôm 20/12 vừa qua đã công bố một báo cáo ghi lại chi tiết các cuộc tấn công phishing, nhắm mục tiêu đến các nhà báo và nhà hoạt động ở Trung Đông và Bắc Phi thông qua việc sử dụng email giả mạo và các trang đăng nhập lấy cắp thông tin khác.

Mục tiêu đằng sau các cuộc tấn công này là lừa để nạn nhân để trao quyền truy cập vào tài khoản Google và Yahoo của họ cho hacker, ngay cả khi họ đã sử dụng xác thực hai yếu tố. “Điều khiến cho cho các cuộc tấn công này trở nên vô cùng phức tạp và hiệu quả chính là cách thức mà chúng lật đổ các chiến lược bảo mật kỹ thuật

số được áp dụng trên các mục tiêu, đây là một quá trình theo kiểu mưa dầm thấm lâu", Amnesty International nhận định trong báo cáo về vụ việc này.

Xác thực hai yếu tố là một biện pháp bảo mật được thiết kế để bảo vệ các tài khoản trực tuyến của bạn trong trường hợp mật khẩu bị đánh cắp. Nó hoạt động với cơ chế: khi bạn cố gắng truy cập vào tài khoản của mình, bạn không chỉ phải nhập thông tin đăng nhập như bình thường mà còn phải cung cấp thêm cả một mã xác thực đặc biệt được gửi qua điện thoại của mình.

Các mật mã đặc biệt được tạo ra bởi hệ thống xác thực hai yếu tố thường chỉ là một chuỗi các số ngẫu nhiên, và đây chính là điểm yếu chí mạng của phương thức bảo mật này, và công việc của tin tặc sẽ là chiếm quyền sử dụng đoạn mã xác thực đó.

Amnesty International cho biết nhóm tin tặc đứng sau vụ tấn công nhắm tới các nhà hoạt động nhân quyền đã loại bỏ xác thực hai yếu tố bằng cách gửi các cảnh báo bảo mật giả mạo nhưng rất có sức thuyết phục, giống như đến từ Google hoặc Yahoo. Các cảnh báo sẽ cho rằng tài khoản của nạn nhân có thể đã bị xâm phạm và cung cấp một liên kết đến trang đăng nhập chính thức để người dùng bắt đầu thiết lập lại mật khẩu. "Đối với hầu hết người dùng, một lời nhắc từ những công ty lớn như Google về việc thay đổi mật khẩu là đủ sức để thuyết phục họ làm theo, và hacker đã nắm bắt và khai thác được tâm lý này của người dùng ", Amnesty International chi sẻ thêm.

Theo Claudio Guarnieri, một chuyên gia công nghệ tại Amnesty International thì về cơ bản, các hacker đã xây dựng một hệ thống 'thí điểm tự động' sẽ khởi chạy Chrome và sử dụng nó để tự động gửi các chi tiết đăng nhập được lấy cắp từ người dùng đến các dịch vụ được chỉ định, bao gồm cả các mã xác minh hai bước được gửi qua SMS.

Quá trình thu thập thông tin tự động của các hacker đóng vai trò rất quan trọng vì nó cho phép chúng nhập mật mã xác thực một lần vào trang đăng nhập Google hoặc Yahoo thực, trước khi mã này hết hạn sử dụng.

Thông thường, những người quan tâm về việc nhận mã xác thực hai yếu tố qua SMS cũng có thể nhận mã thông qua ứng dụng xác thực, chứ không riêng gì SMS, và các mã này được thay đổi cứ sau vài giây. Amnesty International đã không trả lời ngay lập tức câu hỏi của báo giới về việc liệu điều này có ảnh hưởng đến các ứng dụng hay không, nhưng một kỹ thuật viên của tổ chức đã cho biết rằng "cách tiếp cận tương tự có thể được sử dụng để lừa đảo mã từ ứng dụng 2FA như Google Authenticator".

Tổ chức nhân quyền này vẫn khuyến nghị mọi người nên áp dụng xác thực hai yếu tố, nhưng cũng phải biết rằng hệ thống này vẫn có những hạn chế nhất định chứ không hoàn hảo như mọi người vẫn tưởng, vì vậy, đừng dại dột nghĩ rằng mình hoàn toàn an toàn. Ví dụ, các nhóm tin tặc được tài trợ hoàn toàn có đủ tài nguyên cũng như nguồn lực để tạo ra các âm mưu lừa đảo công phu nhằm phá vỡ các biện pháp

bảo vệ hiện nay. Ngoài những kiểu tấn công lừa đảo, chúng cũng có thể cố gắng lây nhiễm phần mềm độc hại cho PC của bạn để đánh cắp thông tin.

"Các cá nhân nằm trong tầm ngắm và những nhà bảo vệ nhân quyền thường là mục tiêu của các cuộc tấn công lừa đảo và điều quan trọng là họ phải được trang bị những kiến thức đúng đắn".

Nếu bạn sẵn sàng rút hầu bao để chi thêm cho vấn đề bảo mật thông tin, bạn cũng có thể đầu tư vào khóa bảo mật để bảo vệ tài khoản trực tuyến của mình. Chúng hoạt động bằng cách thay thế quy trình xác thực hai yếu tố bằng một thiết bị dựa trên phần cứng, và thiết bị này sẽ cần được kết nối với PC của bạn, qua đó giúp đăng nhập vào tài khoản và tài khoản này cũng sẽ được bảo vệ tối ưu hơn. Điểm cộng lớn của khóa bảo mật là rất khó để hacker có thể đánh cắp được, đơn giản bởi nó là một thiết bị phần cứng và để đánh cắp được thì kẻ tấn công phải đích thân đến và lấy nó từ tay bạn. Không phải mọi dịch vụ trực tuyến đều hỗ trợ hình thức bảo mật này, nhưng bạn có thể sử dụng nó để bảo vệ tài khoản của mình trên các dịch vụ phổ biến như Google, Facebook, Dropbox và Twitter.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần kiểm tra các thông tin từ các đường link gửi đến yêu cầu xác thực tài khoản của mình trước khi điền thông tin, đối với các ứng dụng xác thực như Google Authenticator cần cập nhật các phiên bản mới nhất để đảm bảo an toàn thông tin.

Link tham khảo: https://securitybox.vn/7123/hacker-su-dung-tan-cong-phishing-tu-dong-de-pha-vo-bao-mat-2-yeu-to/

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	Orange Livebox	CVE-2018-20377 CVE-2018-20577 CVE-2018-20576 …	Nhóm 04 lỗ hổng trên Orange Livebox (thiết bị giải trí đa năng trên nền tảng hệ điều hành Android dùng nhiều trong hộ gia đình) cho phép đối tượng tấn công thu thập thông tin xác thực thông qua kết nối Wifi (trên cổng 8080), khai thác lỗi CSRF. Ảnh hưởng tới thiết bị có firmware 01.11.2017-11:43:44, Boot v0.70.03, Modem 5.4.1.10.1.1A, Hardware 02, và Arcadyan ARV7519RW22-A-LT VR9 1.2.	Chưa có thông tin xác nhận và bản vá
2	Asus	CVE-2018-18535 CVE-2018-18537 CVE-2018-18536	Nhóm 03 lỗ hổng trên ASUS Aura Sync cho phép đối tượng tấn công thực thi mã lệnh và tấn công leo thang trên hệ thống	Chưa có thông tin xác nhận và bản vá
3	Dlink	CVE-2018-18009 CVE-2018-18007 CVE-2018-18008	Nhóm 05 lỗ hổng trên một số dòng thiết bị D-Link (DSL, DIR, DWR, DCM) cho phép đối tượng tấn công thu thập thông tin xác thực qua nhiều thành phần khác nhau từ đó có thể kiểm soát hệ thống.	Chưa có thông tin xác nhận
4	Epson	CVE-2018-19248 CVE-2018-18960 CVE-2018-19232	Nhóm 04 lỗ hổng trong một số sản phẩm máy in của Epson cho phép đối tượng tấn công đưa tập tin độc hại vào firmware và khởi động lại máy in mà không cần thông tin xác thực.	Chưa có thông tin xác nhận và bản vá
5	Foxit	CVE-2018-20247 CVE-2018-20248 CVE-2018-20249	Nhóm 03 lỗ hổng trên Foxit Quick PDF Library cho phép đối tượng tấn công khai thác	Đã có thông tin xác nhận

			lỗi tràn bộ đệm để chèn và thực thi mã lệnh trên máy tính người dùng	và bản vá
6	SQLite	CVE-2018-20346	Lỗ hổng trên SQLite phiên bản trước 3.25.3 khi bật extension FTS (phần mở rộng của trình duyệt Chrome cho phép người dùng thực hiện một số thao tác với cơ sở dữ liệu) cho phép đối tượng tấn công 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	m5o221fx8.ru
5	xjpakmdcfuqe.com
6	mrkniokqsi.ru
7	kukutrustnet777.info
8	4spo5kkw.ru
9	0-0-0-0-0-0-0-0-0-0-0-0-0-0-5-0-0-0-0-0-0-0-0-0-0-0-0-0.info
10	kukutrustnet987.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.