| STT | Tiêu đề | Nội dung tóm tắt |
|---|---|---|
| **1.** | Citrix cảnh báo rằng tin tặc có thể nhanh chóng khai thác lỗ hổng mới được vá | Citrix đã phát hành bản cập nhật bao gồm nhiều lỗ hổng trong Quản lý điểm cuối Citrix (CEM) còn được gọi là XenMobile. Việc xâu chuỗi các lỗ hổng cho phép kẻ tấn công từ xa chưa được xác thực giành quyền kiểm soát máy chủ Citrix Endpoint Management (CEM). Các lỗ hổng có thể được theo dõi là CVE-2020-8208, CVE-2020-8209, CVE-2020-8210, CVE-2020-8211 và CVE-2020-8212. Phiên bản Citrix bị ảnh hưởng Các tác động của lỗ hổng bảo mật khác nhau giữa các lỗ hổng |
| **2.** | Các lỗi thực thi mã quan trọng với Adobe Acrobat và Reader | Adobe đã phát hành các bản cập nhật sửa chữa 26 lỗ hổng trong các sản phẩm Adobe Acrobat, Reader và Lightroom. Trong số 26 lỗ hổng, 11 lỗ hổng được đánh giá là nghiêm trọng, chúng có thể bị tin tặc lợi dụng để chạy mã tùy ý từ xa hoặc bỏ qua các tính năng bảo mật trên các cài đặt dễ bị tấn công. Adobe Acrobat và Reader \| APSB20-48 Adobe phát hành bảo mật |
| **3.** | Cảnh giác với các kết quả trang đầu Google \| Google Ads | Hãy cảnh giác với các kết quả tìm kiếm đầu tiên của google, một số kẻ tấn công lợi dụng quảng cáo để phát tán các loại mã độc, Adware với các kết quả tìm kiếm hàng đầu. |
| **4.** | Tin tặc lạm dụng Microsoft Teams Updater để cài đặt phần mềm độc hại bằng cách sử dụng kỹ thuật Living off the Land | Một lỗ hổng mới với Microsoft Teams Updater cho phép kẻ tấn công cài đặt và chạy phần mềm độc hại từ một vị trí từ xa bằng cách sử dụng Kỹ thuật sống ngoài đất liền. Vấn đề được tiết lộ lần đầu tiên vào năm ngoái và nó dựa vào việc sử dụng lệnh 'update' để chạy mã nhị phân tùy ý với ngữ cảnh của người dùng hiện tại. Microsoft Teams Updater |
| **5.** | An ninh mạng: Các khuyến nghị để ngăn chặn các cuộc tấn công Bảo mật | Trong thời gian gần đây nhất, chúng tôi thấy có nhiều cuộc tấn công phát sinh ở nhiều tổ chức liên quan đến dữ liệu. Bảo mật dữ liệu là một trong những khía cạnh thiết yếu của một tổ chức vì mọi thứ đều chạy xung quanh dữ liệu. Những ngày này những kẻ tấn công chủ yếu nhắm vào các doanh nghiệp nhỏ. Các doanh nghiệp nhỏ có ít dữ liệu hơn với các mạng kém an toàn hơn.<br><br>Tập trung vào các chính sách an toàn thông tin<br>Có các giải pháp ngăn chặn tấn công<br>Nên có SOC để ngăn chặn sớm các tấn công mà các giải pháp phòng thủ bỏ sót, giảm thiểu các mất mát không đáng có. |
| **6.** | Black Hat USA 2020: Lỗ hổng Wi-Fi nguy hiểm KrØØk Bị ảnh hưởng nhiều chipset wi-fi hơn đã công bố | Các nhà nghiên cứu bảo mật gần đây đã phát hiện ra rằng các chip Wi-Fi nhỏ của Qualcomm và MediaTek dễ bị tấn công bởi các biến thể mới nhất của lỗ hổng tiếp xúc dữ liệu KrØØk. KrØØk là một lỗ hổng khá nguy hiểm và lỗ hổng này hiện đã ảnh hưởng đến nhiều chipset Wi-Fi hơn cho phép giải mã trái phép một số lưu lượng được mã hóa WPA2. Ban đầu, nó được phát hiện vào tháng 2 và số lượng thiết bị ảnh hưởng được công bố là nhỏ hơn so với thực tế. |

| | | |
|---|---|---|
| **7.** | Các tài khoản Reddit bị Hack hàng loạt - Nhiều Subreddits Thỏa thuận Đăng các Thông điệp ủng hộ Trump | Reddit đã bị một vụ hack lớn, nhiều subreddits đã bị xóa trong 24 giờ qua và những kẻ tấn công đã đăng các thông điệp ủng hộ chiến dịch tái tranh cử của Donald Trump. Quản trị viên Reddit kêu gọi người dùng kích hoạt xác thực hai yếu tố (2FA) trên tài khoản của họ và thay đổi mật khẩu của họ. Chiến dịch là một sự cố đang diễn ra với các tài khoản người kiểm duyệt bị xâm phạm và sử dụng |
| **8.** | Cuộc tấn công mới cho phép tin tặc giải mã mã hóa VoLTE để theo dõi cuộc gọi điện thoại | Một nhóm các nhà nghiên cứu - những người trước đây đã gây chú ý vào đầu năm nay vì phát hiện ra các vấn đề bảo mật nghiêm trọng trong mạng 4G LTE và 5G - hôm nay đã trình bày một cuộc tấn công mới có tên là 'ReVoLTE', có thể cho phép những kẻ tấn công từ xa phá vỡ mã hóa được sử dụng bởi các cuộc gọi thoại VoLTE và theo dõi các cuộc điện thoại được nhắm mục tiêu.<br><br>Cuộc tấn công không khai thác bất kỳ lỗ hổng nào trong giao thức Thoại qua LTE (VoLTE) nhưng vẫn có thể nghe lén các cuộc điện thoại. |
| **9.** | Amazon Alexa Bugs cho phép tin tặc cài đặt các kỹ năng độc hại từ xa | Chú ý! Nếu bạn sử dụng trợ lý giọng nói Alexa của Amazon trong loa thông minh của mình, chỉ cần mở một liên kết web trông có vẻ ngây thơ có thể cho phép những kẻ tấn công cài đặt các kỹ năng hack vào đó và theo dõi các hoạt động của bạn từ xa.<br><br>Các nhà nghiên cứu an ninh mạng của Check Point — Dikla Barda, Roman Zaikin và Yaara Shriki — hôm nay đã tiết lộ các lỗ hổng bảo mật nghiêm trọng trong trợ lý ảo Alexa của Amazon có thể hiển thị nó |
| **10.** | Microsoft tiết lộ những cách mới vô tội mà người dùng Windows có thể bị tấn công | Các nhà nghiên cứu an ninh mạng ngày nay đã phát hiện ra modus operandi của một nhóm mối đe dọa khó nắm bắt được các tổ chức ngoại giao và quân sự cao cấp ở Đông Âu để làm gián điệp.<br><br>Những phát hiện này là một phần trong phân tích hợp tác của công ty an ninh mạng ESET và các công ty bị ảnh hưởng, dẫn đến cái nhìn bao quát về hoạt động của InvisiMole và các chiến thuật, công cụ và quy trình của nhóm |
| **11.** | Lỗ hổng quan trọng ảnh hưởng đến quản lý điểm cuối Citrix (Máy chủ XenMobile) | Citrix hôm nay đã phát hành các bản vá cho nhiều lỗ hổng bảo mật mới ảnh hưởng đến Citrix Endpoint Management (CEM), còn được gọi là XenMobile, một sản phẩm dành cho các doanh nghiệp nhằm giúp các công ty quản lý và bảo mật thiết bị di động của nhân viên từ xa.<br><br>Citrix Endpoint Management cung cấp cho các doanh nghiệp khả năng quản lý thiết bị di động (MDM) và quản lý ứng dụng di động (MAM). Nó cho phép |
| **12.** | Lỗi Google Chrome có thể cho phép tin tặc vượt qua bảo vệ CSP; Hãy cập nhật trình duyệt web | Nếu gần đây bạn chưa cập nhật trình duyệt web Chrome, Opera hoặc Edge của mình lên phiên bản mới nhất hiện có, bạn nên làm như vậy càng nhanh càng tốt.<br><br>Các nhà nghiên cứu an ninh mạng vào thứ Hai đã tiết lộ chi tiết về lỗ hổng zero-day trong trình duyệt web dựa trên Chromium dành cho Windows, Mac và Android có thể cho phép kẻ tấn công bỏ qua hoàn toàn các quy tắc của Chính sách bảo mật nội dung (CSP) |

| | | |
|---|---|---|
| **13.** | Lỗ hổng và khai thác vBulletin 0-Day RCE mới được tiết lộ công khai | Một nhà nghiên cứu bảo mật vào đầu ngày hôm nay đã tiết lộ công khai chi tiết và mã khai thác bằng chứng cho một lỗ hổng thực thi mã từ xa zero-day nghiêm trọng chưa được vá, ảnh hưởng đến phần mềm diễn đàn internet được sử dụng rộng rãi vBulletin đã được khai thác PoC.<br><br>vBulletin là một gói phần mềm diễn đàn Internet độc quyền được sử dụng rộng rãi dựa trên máy chủ cơ sở dữ liệu PHP và MySQL. |
| **14.** | Nhà nghiên cứu chứng minh một số lỗ hổng thu phóng ở DEF CON 28 | Ứng dụng hội nghị truyền hình phổ biến Zoom đã giải quyết một số lỗ hổng bảo mật, hai trong số đó ảnh hưởng đến ứng dụng Linux của nó, có thể cho phép kẻ tấn công có quyền truy cập vào hệ thống bị xâm phạm để đọc và lấy dữ liệu người dùng Zoom — và thậm chí chạy phần mềm độc hại lén lút như một quy trình phụ của ứng dụng đáng tin cậy.<br><br>Theo nhà nghiên cứu an ninh mạng Mazin Ahmed, người đã trình bày phát hiện của mình tại DEF CON 28 |
| **15.** | Các lỗ hổng giao thức Internet di động mới cho phép tin tặc nhắm vào người dùng 4G / 5G | Các lỗ hổng tác động cao trong giao thức truyền thông hiện đại được sử dụng bởi các nhà khai thác mạng di động (MNOs) có thể bị khai thác để chặn dữ liệu người dùng và thực hiện các cuộc tấn công mạo danh, lừa đảo và từ chối dịch vụ (DoS), cảnh báo một nghiên cứu mới được công bố.<br><br>Những phát hiện này là một phần của một lỗ hổng mới trong báo cáo LTE và 5G Networks 2020 được công bố bởi công ty an ninh mạng có trụ sở tại London |
| **16.** | Capital One bị phạt 80 triệu đô la cho vụ vi phạm dữ liệu năm 2019 ảnh hưởng đến 106 triệu người dùng | Một cơ quan quản lý Hoa Kỳ đã phạt nhà cung cấp thẻ tín dụng Capital One Financial Corp 80 triệu đô la vì vi phạm dữ liệu năm ngoái làm lộ thông tin cá nhân của hơn 100 triệu người đăng ký thẻ tín dụng của người Mỹ.<br><br>Khoản tiền phạt được đưa ra bởi Văn phòng Kiểm soát Tiền tệ (OCC), một văn phòng độc lập trong Bộ Ngân khố Hoa Kỳ. |
| **17.** | Tin tặc tránh được phát hiện tấn công Credit Card Skimmers sử dụng Homograph Domains và Infected Favicon | Các nhà nghiên cứu an ninh mạng ngày nay đã nêu bật một kỹ thuật lừa đảo lảng tránh mà những kẻ tấn công đang khai thác một cách hoang dã để nhắm mục tiêu vào những khách truy cập của một số trang web có tên miền không chính xác và tận dụng các biểu tượng yêu thích đã được sửa đổi để đưa vào chương trình lướt web điện tử và đánh cắp thông tin thẻ thanh toán một cách bí mật.<br><br>"Ý tưởng rất đơn giản và bao gồm việc sử dụng các ký tự trông giống nhau để đánh lừa người dùng", Malwarebytes |
| **18.** | COVID-19 đã thay đổi các ưu tiên an ninh mạng của doanh nghiệp mãi mãi như thế nào | Trong phần lớn thời gian của năm nay, các chuyên gia CNTT trên toàn cầu đã dốc hết sức lực, tìm cách giúp các doanh nghiệp đối phó với sự bùng phát của đại dịch coronavirus (COVID-19). Trong nhiều trường hợp, nó liên quan đến việc triển khai nhanh chóng cơ sở hạ tầng làm việc từ xa quan trọng. Cơ sở hạ tầng đó đã được đưa vào sử dụng với ít hoặc không có cảnh báo và thậm chí còn ít cơ hội để thử nghiệm. Không cần phải nói, covid đã làm thay đổi cuộc sống của toàn nhân loại. |

| | | |
|---|---|---|
| **19.** | SMBleed: Lỗ hổng nghiêm trọng mới ảnh hưởng đến Giao thức SMB của Windows | Các nhà nghiên cứu bảo mật không gian mạng hôm nay đã phát hiện ra một lỗ hổng nghiêm trọng mới ảnh hưởng đến giao thức SMB (Server Message Block) có thể cho phép kẻ tấn công rò rỉ bộ nhớ kernel từ xa và khi kết hợp với một lỗi "wormable" được tiết lộ trước đó, lỗ hổng có thể bị khai thác để đạt được các cuộc tấn công thực thi mã từ xa .<br>Được đặt tên là "SMBleed" (CVE-2020-1206) bởi công ty an ninh mạng ZecOps, lỗ hổng nằm ở |
| **20.** | Bộ xử lý Intel, ARM, IBM, AMD dễ bị tấn công kênh kề (side-channel) mới | CISA của Hoa Kỳ gần đây đã nhận thấy rằng tin tặc sử dụng Email lừa đảo để triển khai phần mềm độc hại KONNNI với sự trợ giúp của các tài liệu Microsoft word được vũ khí hóa. KONNI RAT ban đầu được tìm thấy vào tháng 5 năm 2017 bởi các nhà nghiên cứu tại nhóm Cisco Talos sau khi nó được vận hành trong các cuộc tấn công nhằm vào các doanh nghiệp có liên kết với Triều Tiên. KONNI<br>Bài đăng của Chính phủ Hoa Kỳ cảnh báo rằng tin tặc sử dụng email lừa đảo được sử dụng để triển khai phần mềm độc hại KONNI bằng tài liệu từ được vũ khí hóa xuất hiện đầu tiên. |
| **21.** | Lỗ hổng trong điện thoại Android Samsung tạo điều kiện cho kẻ tấn công thực hiện Remote Attacks | Nghiên cứu mới đã tiết lộ một loạt lỗ hổng bảo mật nghiêm trọng trong 'Find My Mobile' - một ứng dụng Android được cài đặt sẵn trên hầu hết các điện thoại thông minh Samsung - có thể cho phép những kẻ tấn công từ xa theo dõi vị trí của nạn nhân trong thời gian thực, giám sát các cuộc gọi điện thoại và tin nhắn, và thậm chí xóa dữ liệu được lưu trữ trên điện thoại.<br><br>Nhà cung cấp dịch vụ an ninh mạng Char49 có trụ sở tại Bồ Đào Nha đã tiết lộ những phát hiện của họ về |
| **22.** | Bất kỳ tài khoản DigiLocker Ấn Độ nào cũng có thể được truy cập mà không cần mật khẩu | Chính phủ Ấn Độ cho biết họ đã giải quyết một lỗ hổng nghiêm trọng trong dịch vụ ví tài liệu bảo mật Digilocker có khả năng cho phép kẻ tấn công từ xa vượt qua mật khẩu một lần di động (OTP) và đăng nhập như những người dùng khác.<br><br>Được phát hiện riêng biệt bởi hai nhà nghiên cứu tiền thưởng lỗi độc lập, Mohesh Mohan và Ashish Gahlot, lỗ hổng có thể dễ dàng bị khai thác |
| **23.** | Nhà nghiên cứu chứng minh 4 biến thể mới của cuộc tấn công Smuggling request HTTP | Một nghiên cứu mới đã xác định được bốn biến thể mới của các cuộc tấn công buôn lậu yêu cầu HTTP hoạt động chống lại các máy chủ web thương mại bán sẵn và máy chủ proxy HTTP khác nhau.<br><br>Amit Klein, Phó Giám đốc Nghiên cứu Bảo mật tại SafeBreach, người đã trình bày những phát hiện hôm nay tại hội nghị bảo mật Black Hat, nói rằng các cuộc tấn công làm nổi bật cách các máy chủ web và máy chủ proxy HTTP vẫn còn nhạy cảm với HTTP. |
| **24.** | Các tin tặc tấn công EU từ Trung Quốc, Nga, Triều Tiên bị FBI truy nã | Hội đồng Liên minh châu Âu đã áp đặt các biện pháp trừng phạt lần đầu tiên đối với những cá nhân hoặc thực thể liên quan đến các cuộc tấn công mạng khác nhau nhắm vào công dân châu Âu và các quốc gia thành viên của nó.<br><br>Chỉ thị đã được ban hành để truy nã sáu cá nhân và ba thực thể chịu trách nhiệm hoặc liên quan đến các cuộc tấn công mạng khác nhau, trong đó một số được biết đến công khai là 'WannaCry', 'NotPetya' và ‘Operation Cloud’ |