BẢN TIN NỘI BỘ

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

1. Nghị định 15/NĐ-CP: Chế tài mạnh cho tin giả, tin vu khống

Không gian mạng mang lại nhiều giá trị tích cực, nhưng cũng có thể gây ra nhiều hệ lụy không mong muốn như: người dùng có thể bị xâm phạm đời tư, bị lừa đảo, chiếm đoạt tài sản và nhiều nguy cơ khác. Nếu chủ quan, đơn giản có thể dẫn tới vô tình hoặc cố ý tán phát những thông tin xấu, độc, gây hại cho cộng đồng, xã hội, thậm chí tiếp tay cho các đối tượng chống phá Đảng, Nhà nước.

Một thực tế đáng lo ngại là môi trường mạng đang bị vẩn đục bởi các hành vi thiếu văn hóa, đặc biệt trong giới trẻ. Có thể thấy tràn lan những lời nói tục, chửi thề, phát ngôn gây sốc, những lời bình luận miệt thị, "ném đá" tập thể, những "anh hùng bàn phím"… đặc biệt là thông tin sai sự thật ngày càng gia tăng.

Thời gian qua, lợi dụng diễn biến phức tạp của dịch Covid-19, nhiều cá nhân đưa thông tin không chính xác hoặc bịa đặt, làm nhiễu loạn, gây tâm lý hoang mang, gây khó khăn cho công tác phòng, chống dịch như: "Hà Giang 6 ca mắc mới"; "Khu cách ly thành phố Hà Nội vỡ trận"; "Bệnh nhân thứ 21 có con riêng"; "Ca đầu tiên tử vong"….

Các thế lực thù địch, phản động trong và ngoài nước đã lợi dụng phát tán trên mạng nhiều thông tin sai sự thật, xuyên tạc tình hình dịch bệnh và công tác chỉ đạo, điều hành của Chính phủ, các Bộ, ngành, địa phương trong nỗ lực phòng, chống dịch.

Cho đến nay, cơ quan chức năng đã xác minh, làm việc với gần 700 trường hợp đưa tin sai sự thật; đã có hơn 300 đối tượng trong nước tung tin giả về dịch COVID-19 bị cơ quan chức năng xử lý. Riêng chủ tài khoản có tên là "KOL" đã tung lên gần 300 bài viết với nội dung sai sự thật về dịch bệnh.

Nhằm ngăn ngừa, xử lý những hành vi vi phạm trên môi trường mạng, Chính phủ đã ra Nghị định 174/2013/NĐ-CP có hiệu lực từ 15/1/2014, quy định về hành vi thông tin sai sự thật trên mạng và các mức phạt với người vi phạm, nhưng sự phát triển của thực tiễn đòi hỏi có nghị định thay thế.

Nghị định 15/2020/NĐ-CP thay thế Nghị định 174/2013/NĐ-CP có những thay đổi về mức xử phạt đối với thuê bao di động trả trước dành cho doanh nghiệp viễn thông di động và quy định mức xử phạt vi phạm hành chính đối với các hành vi tung thông tin giả mạo, gây hoang mang dư luận trên mạng xã hội.

Theo đó, Điều 101, quy định phạt tiền từ 10-20 triệu đồng đối với hành vi lợi dụng mạng xã hội để cung cấp, chia sẻ thông tin giả mạo, thông tin sai sự thật, xuyên tạc, vu khống, xúc phạm uy tín của cơ quan, tổ chức, danh dự, nhân phẩm của cá nhân; cung cấp, chia sẻ thông tin bịa đặt, gây hoang mang trong Nhân dân, kích động bạo lực, tội ác, tệ nạn xã hội, đánh bạc hoặc phục vụ đánh bạc.

Các hành vi lợi dụng mạng xã hội để cung cấp, chia sẻ thông tin cổ súy các hủ tục, mê tín, dị đoan, dâm ô, đồi trụy, không phù hợp với thuần phong, mỹ tục của dân tộc; cung cấp, chia sẻ thông tin miêu tả tỉ mỉ hành động chém, giết, tai nạn, kinh dị, rùng rợn cũng bị phạt tiền từ 10-20 triệu đồng.

Mức phạt này cũng áp dụng đối với hành vi lợi dụng mạng xã hội để cung cấp, chia sẻ hình ảnh bản đồ Việt Nam nhưng không thể hiện hoặc thể hiện không đúng chủ quyền quốc gia; quảng cáo, tuyên truyền, chia sẻ thông tin về hàng hóa, dịch vụ bị cấm; cung cấp, chia sẻ đường dẫn đến thông tin có nội dung bị cấm; cung cấp, chia sẻ các tác phẩm báo chí, văn học, nghệ thuật, xuất bản phẩm mà không được sự đồng ý của chủ thể quyền sở hữu trí tuệ hoặc chưa được phép lưu hành hoặc đã có quyết định cấm lưu hành hoặc tịch thu.

Nghị định cũng quy định mức phạt tiền từ 20-30 triệu đồng đối với hành vi tiết lộ thông tin thuộc danh mục bí mật nhà nước, bí mật đời tư của cá nhân và bí mật khác mà chưa đến mức truy cứu trách nhiệm hình sự.

Ngoài ra, Nghị định cũng quy định biện pháp khắc phục hậu quả, buộc gỡ bỏ thông tin sai sự thật hoặc gây nhầm lẫn hoặc thông tin vi phạm pháp luật do thực hiện hành vi vi phạm nêu trên.

Hướng đến lành mạnh hóa môi trường mạng, cần sự chung tay của cả hệ thống chính trị, các tổ chức xã hội và của mỗi người dân.

Nghị định 15/2020/NĐ-CP của Chính phủ là cơ sở pháp lý quan trọng điều chỉnh hành vi cá nhân, tổ chức trên môi trường mạng. Tuy nhiên, điều quan trọng hơn cả là hướng đến lành mạnh hóa môi trường mạng, với sự chung tay của cả hệ thống chính trị, các tổ chức xã hội và của mỗi người dân.

Điều quan trọng trước hết là mỗi người cần nâng cao ý thức, rèn luyện hành vi đạo đức. Khi hoạt động trên không gian mạng cũng phải có suy nghĩ và hành vi ứng xử tương ứng, thống nhất với cuộc sống đời thực, trong tất cả các mối quan hệ, xây dựng thái độ tôn trọng người khác, biết quan tâm, lắng nghe, chia sẻ và cảm thông.

Có trách nhiệm lời nói và hành vi của chính mình; tìm hiểu kỹ các nguồn thông tin để kiểm chứng, không đưa ra những nhận xét, bình luận vội vàng, không đúng hoặc ác ý; không chia sẻ nội dung thông tin xấu, độc. Có ý thức giữ gìn bản sắc văn hóa dân tộc, sự trong sáng của tiếng Việt khi giao tiếp trên mạng.

Mỗi người cần nghiên cứu, tìm hiểu và thực hiện nghiêm Luật An ninh mạng và các quy định trong Nghị định 15/2020/NĐ-CP, nhất là những hành vi bị cấm như những hành vi xúc phạm danh dự, uy tín, nhân phẩm người khác; thông tin bịa đặt, sai sự thật; hoạt động mại dâm, tệ nạn xã hội, phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe cộng đồng.

Tăng cường các biện pháp bảo mật thông tin cá nhân, giữ bí mật mật khẩu, đặt chế độ xem phù hợp; sử dụng phần mềm lọc, ngăn chặn thông tin xấu, độc; tham khảo chuyên gia về cách sử dụng mạng an toàn. Phối hợp chặt chẽ với bộ phận chăm sóc khách hàng mà mình sử dụng dịch vụ, với cơ quan công an để ngăn chặn những hành vi vi phạm và xử lý các tình huống rủi ro phát sinh.

Các cơ quan chức năng sớm ban hành Bộ quy tắc ứng xử trên không gian mạng. Theo đó, cần đưa ra các quy tắc chung như tôn trọng, trách nhiệm, lành mạnh và an toàn; các quy tắc riêng đối với người dùng theo các mức độ khác nhau như: Nên/không nên, được/không được.

Thực hiện tốt Đề án "Xây dựng văn hóa ứng xử trong trường học giai đoạn 2018 - 2025"; tăng cường giáo dục, xây dựng văn hóa ứng xử văn minh, lịch sự, bồi dưỡng các kỹ năng ứng phó với các tình huống trên mạng. Sáng tạo những phong trào tương tự như phong trào "Giờ trái đất", "Mùa hè xanh"...

Cán bộ, đảng viên, thầy cô giáo, các bậc phụ huynh phải mẫu mực về văn hóa, đạo đức, lối sống, có biện pháp quản lý chặt chẽ khi con em tham gia mạng xã hội; có những lời khuyên hữu ích và có những tác động điều chỉnh khi cần thiết.

Cơ quan chuyên trách nghiên cứu thành lập bộ phận chuyên tìm kiếm những bài đăng sai sự thật, xúc phạm người khác, những hình ảnh phản cảm,…gửi tới nhà cung cấp dịch vụ xuyên quốc gia, các mạng xã hội mà người dùng đăng tải và yêu cầu gỡ bỏ.

Link tham khảo: http://antoanthongtin.vn/chinh-sach---chien-luoc/nghi-dinh-15nd-cp-che-tai-manh-cho-tin-gia-tin-vu-khong-106077

2. Hơn 4000 ứng dụng Android để lộ dữ liệu người dùng do cơ sở dữ liệu có sai sót cấu hình

Nhà nghiên cứu Bob Diachenko của Security Discovery đã hợp tác với công ty công nghệ Comparitech để tiến hành một cuộc điều tra trên 15.735 ứng dụng Android, chiếm khoảng 18% tổng số ứng dụng trên cửa hàng Google Play.

Phía Comparitech cho biết "4,8% ứng dụng di động có lưu trữ dữ liệu người dùng trên Google Firebase đã không được bảo mật đúng cách. Ai cũng có thể truy cập vào cơ sở dữ liệu chứa thông tin cá nhân của người dùng, mã thông báo truy cập và các dữ liệu khác mà không cần mật khẩu hoặc bất kỳ phương thức xác thực nào khác".

Được Google mua lại vào năm 2014, Firebase là một nền tảng phát triển ứng dụng di động phổ biến, cung cấp nhiều công cụ để giúp các nhà phát triển xây dựng ứng dụng, lưu trữ dữ liệu và tệp ứng dụng một cách an toàn, khắc phục sự cố và thậm chí kết nối với người dùng qua tin nhắn của ứng dụng.

Các ứng dụng bị mắc lỗi chủ yếu là các ứng dụng về trò chơi, giáo dục, giải trí và kinh doanh. Tổng lượt cài đặt của các ứng dụng trên là 4,22 tỷ lần và "rất có thể quyền riêng tư của người dùng Android đã bị xâm phạm bởi ít nhất một ứng dụng".

Vì Firebase là một công cụ đa nền tảng nên các nhà nghiên cứu cũng cảnh báo rằng những cấu hình lỗi cũng có khả năng ảnh hưởng đến iOS và các ứng dụng trên web.

Những thông tin bị ảnh hưởng trên 4.282 ứng dụng bao gồm:

Địa chỉ email: 7.000.000+

Tên người dùng: 4.400.000+

Mật khẩu: 1.000.000+

Số điện thoại: 5.300.000+

Tên đầy đủ: 18.300.000+

Tin nhắn trò chuyện: 6.800.000+

Dữ liệu GPS: 6.200.000+

Địa chỉ IP: 156.000+

Địa chỉ theo tên đường phố: 560.000+

Diachenko nhận thấy các cơ sở dữ liệu sử dụng REST API của Firebase để truy cập dữ liệu được lưu trữ trên các thực thể không được bảo vệ, chúng được truy xuất ở định dạng JSON, bằng cách thêm "/.json" vào URL cơ sở dữ liệu (ví dụ: https://~project_id~.firebaseio.com/.json).

Ngoài 155.066 ứng dụng công khai cơ sở dữ liệu, các nhà nghiên cứu đã tìm thấy 9.014 ứng dụng cung cấp quyền ghi, cho phép kẻ tấn công chèn dữ liệu độc hại và làm hư hỏng cơ sở dữ liệu và thậm chí phát tán phần mềm độc hại.

Một vấn đề phức nữa là việc lập chỉ mục cho các URL cơ sở dữ liệu của Firebase trên các công cụ tìm kiếm như Bing sẽ để lộ các endpoints có chứa lỗi cho bất kỳ ai trên Internet. Tìm kiếm trên Google cũng không đưa ra kết quả.

Sau khi được thông báo về sự việc vào ngày 22 tháng 4, Google cho biết họ sẽ liên hệ với các nhà phát triển bị ảnh hưởng để khắc phục các vấn đề.

Đây không phải là lần đầu tiên Firebase bị rò rỉ thông tin cá nhân. 2 năm trước, các nhà nghiên cứu từ công ty bảo mật di động Appthority đã tìm thấy một vụ để lộ dữ liệu tương tự ảnh hưởng đến 100 triệu hồ sơ dữ liệu.

Để một cơ sở dữ liệu mở công khai, không có bất kỳ phương thức xác thực nào là một lời mời chào đến những kẻ xấu. Vì thế, các nhà phát triển ứng dụng nên tuân thủ các quy tắc cơ sở dữ liệu của Firebase để bảo mật dữ liệu và ngăn chặn việc truy cập trái phép.

Người dùng được khuyến khích chỉ sử dụng các ứng dụng đáng tin cậy và thận trọng về thông tin được chia sẻ với một ứng dụng.

Khuyến nghị: Người dùng cần tìm hiểu kỹ trước khi sử dụng các ứng dụng trên thiết bị di động, tránh để lộ các thông tin nhạy cảm để bảo đảm an toàn thông tin.

Link tham khảo: https://securitydaily.net/hon-4000-ung-dung-android-de-lo-du-lieu-nguoi-dung-do-co-so-du-lieu-co-sai-sot-cau-hinh/

3. Patch Tuesday tháng 5 của Microsoft vá 111 lỗ hổng

Không có lỗ hổng nào đã bị công khai hoặc đang bị khai thác tại thời điểm phát hành.

Ngoài bản vá cho bộ nhớ đệm của hệ điều hành, trình duyệt, Office và SharePoint, Microsoft cũng phát hành bản cập nhật cho .NET Framework, .NET Core, Visual Studio, Power BI, Windows Defender và Microsoft Dynamics.

Lỗ hổng nâng cao đặc quyền

Phần lớn bản vá dành cho các lỗi leo thang đặc quyền có mức độ quan trọng. Có tất cả 56 bản vá lỗi này trong bản cập nhật tháng này, chủ yếu dành cho Windows. Kẻ tấn công, có thể khai thác lỗ hổng sau khi truy cập vào hệ thống để thực thi mã trên hệ thống mục tiêu với đặc quyền leo thang.

Theo chuyên gian Narang của công ty Tenable, ba lỗi sau đây nhiều khả năng có thể bị khai thác: Hai lỗ hổng trong Win32k (CVE-2020-1054, CVE-2020-1143) và một lỗ hổng trong đồ họa của Windows (CVE-2020-1135).

Theo Microsoft, cả hai lỗ hổng trong Win32k bắt nguồn từ việc driver (trình điều khiển) kernel-mode của Windows không xử lý chính xác các đối tượng trong bộ nhớ. Hacker khi khai thác thành công lỗ hổng có thể chạy mã tùy ý trong kernel-mode, từ đó có thể cài đặt các chương trình, xem, thay đổi hoặc xóa dữ liệu hoặc tạo tài khoản mới với quyền người dùng đầy đủ.

Để khai thác lỗ hổng, trước tiên kẻ tấn công phải đăng nhập vào hệ thống, sau đó chạy một ứng dụng đặc biệt để khai thác lỗ hổng và kiểm soát hệ thống bị ảnh hưởng.

Trong khi đó, lỗi leo thang đặc quyền của đồ họa Windows (trong phần lớn Windows 10 và Windows Server) có thể bị hacker lợi dụng để nâng cao đặc quyền trong tiến trình nhằm đánh cắp thông tin xác thực hoặc dữ liệu nhạy cảm, tải xuống phần mềm độc hại hoặc thực thi mã độc.

Ngoài ra, tồn tại một lỗi leo thang đặc quyền nghiêm trọng trong Microsoft Edge (CVE-2020-1056). Theo Microsoft, lỗ hổng bắt nguồn từ việc Edge không thực thi đúng các chính sách tên miền chéo, có thể cho phép kẻ tấn công truy cập thông tin từ một tên miền và inject thông tin vào một tên miền khác. Tuy nhiên, tấn công đòi hỏi phải có sự tương tác của người dùng, như lừa người dùng click vào một liên kết dẫn đến trang web của kẻ tấn công.

Theo kịch bản tấn công, kẻ tấn công có thể lưu trữ (host) một trang web được sử dụng để khai thác lỗ hổng an ninh. Ngoài ra, các trang web bị tấn công và trang web chấp nhận hoặc lưu trữ nội dung do người dùng cung cấp chứa nội dung đặc biệt có thể khai thác lỗ hổng.

Các bản vá nghiêm trọng cần xem xét

Các lỗ hổng đáng chú ý khác bao gồm hai lỗi thực thi mã từ xa (RCE) trong Microsoft Color Management (CVE-2020-1117) và Windows Media Foundation (CVE-2020-1126). Cả hai lỗ hổng đều có thể bị khai thác bằng cách lừa người dùng mở file độc hại đính kèm email hoặc truy cập trang web có chứa mã khai thác.

Theo chuyên gia Narang, khai thác thành công sẽ cho phép kẻ tấn công có được các quyền thao tác trên hệ thống tương tự quyền người dùng hiện tại. Nếu người dùng là quản trị, hacker có thể thực hiện nhiều thao tác như cài đặt chương trình, tạo tài khoản mới với toàn quyền người dùng và xem, thay đổi hoặc xóa dữ liệu.

Các lỗ hổng nghiêm trọng trong Chakra Core, Internet Explorer, EdgeHTML và SharePoint cũng được cập nhật bản vá. Trong đó SharePoint có bốn lỗi nghiêm trọng, tiếp tục là sản phẩm có nhiều lỗi nhất so với tháng trước.

Hầu hết các lỗ hổng nghiêm trọng đều được xử lý bằng cách cập nhật hệ điều hành và trình duyệt, nhưng có bốn lỗ hổng nghiêm trọng trong SharePoint và một trong Visual Studio, chuyên gia an ninh Todd Schell của công ty Ivanti cho biết.

Hai lỗ hổng CVE-2020-1023 và CVE-2020-1102 trên SharePoint là các lỗ hổng RCE có mức độ quan trọng cho phép hacker truy cập hệ thống và đọc hoặc xóa nội dung, thay đổi hoặc chạy trực tiếp mã trên hệ thống.

Điều này không chỉ cho phép kẻ tấn công truy cập nhanh chóng và dễ dàng vào các dữ liệu quan trọng nhất được lưu trữ trong máy chủ SQL của một tổ chức mà còn là nền tảng để thực hiện các cuộc tấn công mới vào các thiết bị khác trong môi trường của tổ chức đó.

Một lỗ hổng khác CVE-202-1024 trong SharePoint cho phép kẻ tấn công thực thi mã tùy ý từ nhóm ứng dụng SharePoint và tài khoản máy chủ SharePoint, có khả năng ảnh hưởng đến tất cả người dùng kết nối và sử dụng nền tảng.

Nếu hacker có thể truy cập vào thành phần quan trọng này, thao tác di chuyển bên trong các hệ thống file được kết nối sẽ khó kiểm soát. Vì số người sử dụng Microsoft SharePoint để làm việc từ xa đang tăng lên, cần nhanh chóng vá lỗ hổng nghiêm trọng này để đảm bảo truy cập vào mạng và dữ liệu của công ty.

Đối với Visual Studio, những người dùng của Studio Code Python Extension cần lưu ý đến hai bản vá được phát hành trong tháng này. Cả hai đều là lỗ hổng RCE. Lỗ hổng CVE-2020-1192 được đánh giá là nghiêm trọng trong khi lỗi CVE-2020-1171 còn lại ở mức độ quan trọng. Theo chuyên gia Childs, không có dấu hiệu nào cho thấy lỗi này nghiêm trọng hơn lỗi kia và người dùng nên xem cả hai là nghiêm trọng.

Các lỗi khác cần chú ý

Quản trị viên cũng nên chú ý đến một số lỗ hổng khác, như hai lỗ hổng VBScript (CVE-2020-1060 và CVE-2020-1058).

Cả hai lỗ hổng có thể cho phép kẻ tấn công có được quyền giống như người dùng hiện tại.

Theo ông Chris Hass, giám đốc nghiên cứu và bảo mật thông tin của công ty Automox dù cả hai lỗ hổng CVE-2020-1058 và CVE-2020-1060 đều không được đánh giá là nghiêm trọng, rất có thể sẽ bị hacker khai thác trên thực tế. Cả hai lỗ hổng đều ảnh hưởng đến VBScript và cách thức công cụ kịch bản này xử lý các đối tượng trong bộ nhớ. Do tính linh hoạt của VBScript trong Windows, có rất nhiều phương thức tấn công có thể bị hacker lợi dụng để khai thác.

Ví dụ, kẻ tấn công có thể lưu trữ một trang web độc hại với payload đặc biệt để khai thác bất kỳ người dùng nào truy cập trang bằng Internet Explorer, inject mã vào trang web bị xâm nhập hoặc thậm chí khởi chạy một chiến dịch quảng cáo độc hại để phục vụ payload thông qua các quảng cáo độc hại trên các trang web phổ biến.

Ngoài ra, còn có một lỗ hổng từ chối dịch vụ (CVE-2020-1118) trong Microsoft Windows Transport Layer Security. Lỗ hổng cho phép kẻ tấn công từ xa khởi động lại để tấn công từ chối dịch vụ.

Phân tích về lỗ hổng an ninh của con trỏ NULL trong quá trình thực thi Windows của giao thức Diffie-Hellman, chuyên gia Childs cho biết kẻ tấn công có thể khai thác lỗ hổng này bằng cách gửi tin nhắn Client Key Exchange độc hại trong quá trình handshake TLS. Lỗ hổng ảnh hưởng đến cả máy khách và máy chủ TLS, do đó, kẻ tấn công có thể làm sập bất kỳ hệ thống nào.

Chuyên gia Melick cũng cho biết lỗi nghiêm trọng trong Visual Studio Code, bắt nguồn từ cách thức tiện ích mở rộng Python tải cài đặt từ file ghi chép, nên là ưu tiên hàng đầu, vì đây là một trong những công cụ môi trường phổ biến nhất dành cho nhà phát triển.

Đây là công cụ chiếm hơn 50% thị phần các công cụ dành cho nhà phát triển, hacker có rất nhiều mục tiêu tiềm năng và nếu thành công, sẽ có khả năng kiểm soát máy nạn nhân như người dùng hiện tại. Theo chuyên gia Melick, một khi giành được quyền truy cập, hacker có thể đánh cắp thông tin quan trọng như mã nguồn, chèn mã độc hoặc cài backdoor vào các dự án hiện tại và cài đặt, sửa đổi hoặc xóa dữ liệu. Do tầm quan trọng và tính phổ biến của Visual Studio Code, các tổ chức cần cập nhật bản vá này trong vòng 24 giờ trước khi lỗ hổng có thể bị khai thác.

Đây là tháng thứ 3 liên tiếp Microsoft phát hành bản vá cho hơn 110 lỗ hổng.

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

Link tham khảo: https://whitehat.vn/threads/patch-tuesday-thang-5-cua-microsoft-va-111-lo-hong.13603/

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 2020 3318 CVE 2020 3313 CVE 2020 3329 ...	Nhóm 35 lỗ hổng trên thiết bị của Cisco (FMC, IMC,..) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã tùy ý, tấn công giả mạo (XSS), tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá.
2	Linux	CVE 2020 12659 CVE 2020 12654 CVE 2020 12653 …	Nhóm 15 lỗ hổng trong hệ điều hành Linux (Linux kernel) cho phép đối tượng tấn công thu thập thông tin, tấn công từ chối dịch vụ	Đã có thông tin xác nhận và bản vá
3	IBM	CVE 2020 7645 CVE 2020 4429 CVE 2020 4427 …	Nhóm 09 lỗ hổng trong các sản phẩm của IBM (Data Risk Manager, …) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã, tấn công XSS. 01 lỗ hổng có điểm CVSS: 10.0 (đặc biệt nghiêm trọng).	Đã có thông tin xác nhận và bản vá
4	Wordpress	CVE-2020-12104 CVE-2020-11727 CVE-2020-8799 …	Nhóm 05 lỗ hổng trong phần mềm Wordpress (WTI Like Post plugin, Wp- advanced-search plugin, …) cho phép đối tượng tấn công tấn công giả mạo XSS, tấn công SQL injection.	Đã có thông tin xác nhận và bản vá
5	Tp-link	CVE-2020-12475 CVE-2020-12110 CVE-2020-12109 …	Nhóm 05 lỗ hổng trong các thiết bị Tp-link (NC260, TL-WA855RE, NC450, …) cho phép đối tượng tấn công chèn và thực thi mã từ xa.	Đã có thông tin xác nhận và bản vá
6	Netgear	CVE-2017-18867 CVE-2017-18864 CVE-2017-18866 …	Nhóm 04 lỗ hổng trong các thiết bị của Netgear (D6100, D7800, R7100LG,…) cho phép đối tượng tấn công tấn công giả mạo XSS.	Đã có thông tin xác nhận và bản vá

7	Apache	CVE-2020-1961 CVE-2020-1959 CVE-2019-17557	Nhóm 03 lỗ hổng trong một số thành phần của Apache (Apache Syncope phiên bản trước 2.0.15 và trướ c 2.1.6) cho phép đối tượng tấn công chèn và thực thi mã từ xa.	Đã có thông tin xác nhận và bản vá
8	Google	CVE-2020-7645 CVE-2020-8896 CVE-2018-21233	Nhóm 03 lỗ hổng trong phần mềm của Google (Google Chrome, TensorFlow,…) cho phép đối tượng tấn công chèn và thực thi mã từ xa.	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	iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
5	ydbnsrt.me
6	tttta.sssaaaas.io
7	cityofangelsmagazine.com
8	track.sayggggames.io
9	xjpakmdcfuqe.in
10	xjpakmdcfuqe.ru

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.