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

1. Hệ thống thông tin báo cáo Chính phủ: Nhiều lợi ích của "số hóa" báo cáo giấy

Chiều 10/3/2020, Bộ trưởng, Chủ nhiệm Văn phòng Chính phủ Mai Tiến Dũng chủ trì cuộc họp với các Bộ, ngành liên quan để chuẩn bị công bố vận hành một số phân hệ của Hệ thống thông tin báo cáo (HTTTBC) Chính phủ.

Theo Cục Kiểm soát thủ tục hành chính, Văn phòng Chính phủ (VPCP), thời gian qua, Cục đã chủ trì, phối hợp với Sáng kiến Việt Nam, Tập đoàn VNPT và các đơn vị liên quan chủ động triển khai xây dựng HTTTBC Chính phủ kết nối với các HTTTBC của Bộ, ngành, địa phương, từ đó hình thành HTTTBC quốc gia.

HTTTBC Chính phủ thu thập, tích hợp dữ liệu báo cáo của các cơ quan hành chính Nhà nước, nhằm tổng hợp, phân tích dữ liệu, phục vụ công tác chỉ đạo, điều hành của Chính phủ, Thủ tướng Chính phủ. Hệ thống nhằm bảo đảm gắn kết chặt chẽ giữa đổi mới lề lối phương thức làm việc với ứng dụng công nghệ thông tin (CNTT) trong công tác phục vụ sự chỉ đạo, điều hành của Chính phủ, Thủ tướng Chính phủ. Đồng thời tăng cường công khai, minh bạch, nâng cao trách nhiệm giải trình của các cơ quan hành chính Nhà nước trong việc cung cấp thông tin, dữ liệu phục vụ sự chỉ đạo, điều hành của Chính phủ, Thủ tướng Chính phủ.

Bên cạnh đó, HTTTBC Chính phủ giúp nâng cao năng lực tham mưu tổng hợp của VPCP trong công tác phục vụ sự chỉ đạo, điều hành của Chính phủ, Thủ tướng Chính phủ.

Mục tiêu đặt ra của HTTTBC Chính phủ nhằm đổi mới, nâng cao hiệu quả ứng dụng CNTT trong công tác tham mưu, tổng hợp, báo cáo; góp phần chuyển đổi phương thức chỉ đạo, điều hành dựa trên dữ liệu số được tổng hợp, phân tích theo thời gian thực, hiển thị trực quan thông qua các hệ thống thông tin, bảng hiển thị.

Theo đó, năm 2020 sẽ kết nối HTTTBC Chính phủ với 100% các hệ thống báo cáo của các Bộ, ngành, địa phương hoặc hệ thống thông tin chuyên ngành có khả năng trích xuất số liệu báo cáo để hình thành HTTTBC quốc gia. Đến năm 2025, mục tiêu có 100% báo cáo định kỳ do bộ, ngành, địa phương báo cáo Chính phủ, Thủ tướng Chính phủ (không bao gồm nội dung mật), 100% báo cáo trong Bộ chỉ tiêu tổng hợp báo cáo định kỳ, báo cáo thống kê về kinh tế-xã hội được gửi, nhận qua HTTTBC Chính phủ...

Tại cuộc họp, Cục Kiểm soát thủ tục hành chính nêu lên những lợi ích của HTTTBC Chính phủ như: Giả sử một báo cáo quy định đối với địa phương thực hiện từ cấp xã đến cấp huyện, lên cấp tỉnh; đối với các Bộ, cơ quan ngang Bộ tổng hợp báo cáo từ các đơn vị trực thuộc và đơn vị ngành dọc gửi Bộ, cơ quan theo chức năng, nhiệm vụ được giao để tổng hợp báo cáo Chính phủ, Thủ tướng… nếu điện tử hóa, hệ thống tổng hợp, thì người có trách nhiệm của mỗi cấp báo cáo chỉ xem và bấm duyệt, gửi báo cáo, mà không phải tổng hợp. Vì thế, thời gian tiết kiệm được cho

bước tổng hợp ước tính là 6/10 ngày, số ngày công tiết kiệm được là 4.752 ngày công/năm.

Theo số liệu do các Bộ, cơ quan cung cấp, bình quân hàng năm mỗi Bộ, cơ quan có khoảng 20 báo cáo định kỳ gửi Chính phủ, Thủ tướng Chính phủ. Như vậy, ước tính tổng số 22 Bộ, cơ quan báo cáo lên Chính phủ, Thủ tướng Chính phủ là 440 báo cáo/năm.

Tính toán của Cục Kiểm soát thủ tục hành chính cho thấy, nếu điện tử hóa tất cả các báo cáo này và kết nối với HTTTBC Chính phủ, thì sẽ tiết kiệm được cho ngân sách Nhà nước khoảng 460 tỷ đồng/năm.

Số liệu báo cáo này chưa tính cho báo cáo chuyên đề, đột xuất, chưa tính số báo cáo các tổ chức, cá nhân ngoài Nhà nước phải báo cáo cơ quan Nhà nước… do Hệ thống bước đầu chỉ triển khai tới các cơ quan hành chính Nhà nước.

Hiện nay, có 9 Bộ, cơ quan đã kết nối với HTTTBC Chính phủ. Cục Kiểm soát tục hành chính cùng các đơn vị liên quan đang tiếp tục kết nối với các Bộ, ngành, địa phương khác triển khai kết nối với hệ thống thông tin dữ liệu chuyên ngành.

Cũng theo Cục Kiểm soát thủ tục hành chính, dự kiến ngày 13/3 tới sẽ ra mắt bước 1 của HTTTBC Chính phủ và dự kiến trong tháng 10/2020 ra mắt HTTTBC quốc gia.

Tại cuộc họp, đại biểu thuộc các bộ, ngành đánh giá đề án HTTTBC Chính phủ rất thiết thực trong giai đoạn hiện nay, quan trọng hơn nữa là nhằm phục vụ công tác chỉ đạo điều hành của Chính phủ, Thủ tướng Chính phủ. Hệ thống khi vận hành sẽ tiết kiệm chi phí, thời gian, đặc biệt là cung cấp số liệu phục vụ cho chiến lược chỉ đạo, điều hành của Chính phủ. Đây cũng là nội dung triển khai kịp thời trong quá trình xây dựng Chính phủ điện tử, hướng tới Chính phủ số.

Bộ trưởng Mai Tiến Dũng thay mặt VPCP tiếp thu toàn bộ ý kiến của các đại biểu về nội dung, giao diện, thiết kế... để hoàn thiện HTTTBC Chính phủ. Theo đó, một số phân hệ của HTTTBC Chính phủ sẽ khai trương ngày 13/3/2020 và hoàn thiện dần, bám vào các chỉ tiêu vĩ mô để tạo ra các hệ thống báo cáo tổng hợp, phục vụ chỉ đạo điều hành của Chính phủ, Thủ tướng Chính phủ.

Bộ trưởng, Chủ nhiệm VPCP đề nghị các bộ, cơ quan chú ý việc chuẩn hóa báo cáo, phân công trách nhiệm cụ thể trong đơn vị để quyết tâm đưa HTTTBC Chính phủ vào vận hành, số hóa các văn bản giấy, tiết kiệm thời gian, chi phí cho ngân sách Nhà nước.

Link tham khảo: http://antoanthongtin.vn/an-toan-thong-tin/he-thong-thong-tin-bao-cao-chinh-phu-nhieu-loi-ich-cua-so-hoa-bao-cao-giay-105902

2. Microsoft tung bản vá khẩn cấp cho Windows 10

Microsoft mới đây phát hành bản vá khẩn cấp cho một lỗ hổng bảo mật vô tình bị lộ ra trong quá trình phát hành bản vá tháng 3.2020 vài ngày trước.

Theo Engadget, mặc dù khó bị khai thác nhưng lỗ hổng này rất "nghiêm trọng" vì nó có thể cho phép mã độc tự động lây lan từ máy này sang máy khác. Microsoft

phát hành bản sửa lỗi ngay lập tức, đặt mục tiêu tránh một phản ứng dây chuyền tương tự xảy ra với virus WannaCry và NotPetya trong năm 2017.

Lỗ hổng bảo mật này tồn tại trong giao thức SMB của Microsoft trên các phiên bản 32 và 64 bit gần đây của Windows 10 ở cả máy trạm và máy chủ. Các nhà nghiên cứu từ Microsoft và nhiều nơi khác đã dán nhãn "quan trọng" cho lỗ hổng này vì chỉ cần một máy bị khai thác có thể dẫn đến những máy khác trên cùng hệ thống mạng gặp nguy hiểm. Microsoft cho biết đến nay không có bằng chứng nào cho thấy lỗ hổng đang được khai thác.

Hãng trích dẫn rằng "kẻ tấn công khai thác thành công lỗ hổng có thể có được khả năng thực thi mã trên máy chủ hoặc máy trạm mục tiêu. Để khai thác lỗ hổng ở góc độ máy chủ, kẻ tấn công không được xác thực có thể gửi một gói tin đặc biệt đến máy chủ SMBv3 đã được nhắm mục tiêu. Để khai thác lỗ hổng ở góc độ máy trạm, kẻ tấn công không được xác thực sẽ cần phải cấu hình máy chủ SMBv3 nhiễm độc và thuyết phục người dùng kết nối với nó".

Windows 10 có khả năng phòng thủ mạnh mẽ khiến kịch bản này khó xảy ra nhưng những kẻ tấn công có động lực và kỹ năng cao có thể sẽ tạo ra các cuộc tấn công thành công. Để ngăn chặn điều đó, người dùng nên cài đặt bản cập nhật bảo mật KB4551762 càng sớm càng tốt thông qua Windows Update.

Khuyến nghị: Người quản trị và người dùng Windows 10 cần cập nhật bản vá mới nhất để đảm bảo an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/microsoft-tung-ban-va-khan-cap-cho-windows-10-1195653.html

3. VMware vá lỗ hổng thực thi mã trong VMware Workstation/Fusion

VMware vừa phát hành các bản cập nhật cho các sản phẩm phần mềm Workstaton và Fusion của mình để xử lý vấn đề an ninh nghiêm trọng, cho phép kẻ tấn công thực thi mã hoặc từ chối dịch vụ trên máy chủ (host) bằng cách sử dụng lỗi trong dịch vụ Windows vmnetdhcp tồn tại trong các phiên bản Vmware và Fusion.

Lỗ hổng này được đánh số CVE-2020-3947 với thang điểm CVSSv3 là 9.3, cho thấy mức độ nghiêm trọng của lỗ hổng này. Lỗ hổng này nằm trong dịch vụ Windows vmnetdhcp, được sử dụng để gán địa chỉ IP cho máy khách thông qua DHCP. Theo lời khuyên của VMware, lỗ hổng này có thể cho phép kẻ tấn công thực hiện một cuộc tấn công từ chối dịch vụ hoặc thực thi các lệnh trên máy chủ Windows.

Nếu khai thác thành công lỗ hổng này có thể tạo điều kiện cho kẻ xấu chiếm quyền kiểm soát tất các các máy ảo (guest) khác thậm chí chiếm quyền điều khiển máy tính có cài phần mềm Vmware và Fusion.

Do tính chất nghiêm trọng của lỗ hổng này, chúng tôi khuyên người dùng nên nâng cấp VMware Workstation càng sớm càng tốt. Các sản phẩm của VMware bị ảnh hưởng bao gồm

- VMware Workstation Pro / Player (Workstation)
- VMware Fusion Pro / Fusion (Fusion)
- VMware Horizon Client for Windows

- VMware Remote Console for Windows (VMRC for Windows)

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

Link tham khảo: https://whitehat.vn/threads/vmware-va-lo-hong-thuc-thi-ma-trong-vmware-workstation-fusion.13345/

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	Apple	CVE-2019-8741	01 lỗ hổng trên sản phẩm của Apple cho phép đối tượng tấn công tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá.
2	Cisco	CVE 2020 3176 CVE 2020 3127 CVE 2020 3181 …	Nhóm 13 lỗ hổng trên thiết bị của Cisco (Cisco Advanced Malware Protection,…) cho phép đối tượng tấn công thu thập thông tin, tấn công XSS, chèn và thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá
3	D-link	CVE 2019 19223 CVE 2019 20501 CVE 2019 20499 …	Nhóm 13 lỗ hổng trên thiết bị D link (D-link DWL-2600AP 4.2.0.15 Rev…) cho phép đối tượng tấn công tấn chèn và thực thi mã từ xa.	Đã có thông tin xác nhận và bản vá
4	Wordpress	CVE 2020 9372 CVE 2020 9456 CVE 2020 9458 …	Nhóm 09 lỗ hổng trên phần mềm Wordpress (the Appointment Booking Calendar plugin, the RegistrationMagic plugin,…) cho phép đối tượng tấn công chèn và thực thi mã tùy ý, tấn công CSV injection.	Đã có thông tin xác nhận và bản vá
5	Qualcomm	CVE 2019 14061 CVE 2018 11838 CVE 2019 14086 …	Nhóm 47 lỗ hổng trên sản phẩm của Qualcomm (Snapdragon Industrial IOT Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon IoT,…) cho phép đối tượng tấn công chèn và thực thi mã tùy ý, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
6	Facebook	CVE 2020 1893 CVE 2020 1888 CVE 2020 1892	Nhóm 03 lỗ hổng trên Facebook (JSON in TryParse,…) cho phép đối	Đã có thông tin xác nhận và

			tượng tấn công tấn công thu thập thông tin, tấn công DOS.	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	track.saygggggames.io
8	xdqzpbcgrvkj.ru
9	xjpakmdcfuqe.in
10	xjpakmdcfuqe.com

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.