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

1. Quy định về Phạm vi bí mật nhà nước cần được bảo vệ

Luật bảo vệ bí mật nhà nước quy định phạm vi bí mật nhà nước là giới hạn thông tin quan trọng trong một số lĩnh vực chưa công khai, nếu bị lộ, bị mất có thể gây nguy hại đến lợi ích quốc gia, dân tộc.

Theo đó, nội dung điều 7 được xây dựng trên cơ sở phân loại lĩnh vực theo quy định tại Luật Tổ chức Chính phủ. Đây cũng là kết quả nghiên cứu, rà soát nội dung bí mật nhà nước tại 96 danh mục bí mật nhà nước hiện hành. Mặt khác, trong quá trình xây dựng, nội dung này cũng đã xin ý kiến từ các bộ, cơ quan ngang bộ và các cơ quan, tổ chức ở trung ương có liên quan trực tiếp đến việc lập danh mục bí mật nhà nước và đạt được sự đồng thuận cao của các cơ quan, tổ chức.

Trên cơ sở phạm vi bí mật nhà nước và phân loại bí mật nhà nước quy định tại Luật Bảo vệ bí mật nhà nước, Thủ tướng Chính phủ sẽ ban hành danh mục cụ thể về bí mật nhà nước theo trình tự, thủ tục chặt chẽ. Cụ thể, Luật Bảo vệ bí mật nhà nước quy định phạm vi bí mật nhà nước giới hạn trong 15 lĩnh vực sau:

Thông tin về chính trị: Chủ trương, chính sách của Đảng và Nhà nước về đối nội, đối ngoại; Hoạt động của Ban Chấp hành Trung ương, Bộ Chính trị, Ban Bí thư và lãnh đạo Đảng, Nhà nước; Chiến lược, đề án về dân tộc, tôn giáo và công tác dân tộc, tôn giáo liên quan đến bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội; Thông tin có tác động tiêu cực đến tình hình chính trị, kinh tế - xã hội.

Thông tin về quốc phòng, an ninh, cơ yếu: Chiến lược, kế hoạch, phương án, hoạt động bảo vệ Tổ quốc, phòng thủ đất nước, bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội; chương trình, dự án, đề án đặc biệt quan trọng; Tổ chức và hoạt động của lực lượng vũ trang nhân dân, lực lượng cơ yếu; Công trình, mục tiêu về quốc phòng, an ninh, cơ yếu; các loại vũ khí, khí tài, phương tiện quyết định khả năng phòng thủ đất nước, bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội; sản phẩm mật mã của cơ yếu.

Thông tin về lập hiến, lập pháp, tư pháp: Hoạt động lập hiến, lập pháp, giám sát, quyết định vấn đề quan trọng của đất nước; Thông tin về khởi tố; công tác điều tra, thực hành quyền công tố, kiểm sát hoạt động tư pháp, xét xử, thi hành án hình sự.

Thông tin về đối ngoại: Chiến lược, kế hoạch, đề án phát triển quan hệ với nước ngoài, tổ chức quốc tế hoặc chủ thể khác của pháp luật quốc tế; tình hình, phương án, kế hoạch, hoạt động đối ngoại của cơ quan Đảng, Nhà nước; Thông tin, thỏa thuận được trao đổi, ký kết giữa Việt Nam với nước ngoài, tổ chức quốc tế hoặc chủ thể khác của pháp luật quốc tế; Thông tin bí mật do nước ngoài, tổ chức quốc tế hoặc chủ thể khác của pháp luật quốc tế chuyển giao theo điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên và thỏa thuận quốc tế có liên quan.

Thông tin về kinh tế: Chiến lược, kế hoạch đầu tư và dự trữ quốc gia bảo đảm quốc phòng, an ninh; đấu thầu phục vụ bảo vệ an ninh quốc gia; Thông tin về tài chính, ngân sách, ngân hàng; phương án, kế hoạch thu, đổi, phát hành tiền; thiết kế

mẫu, chế tạo bản in, khuôn đúc, công nghệ in, đúc tiền và giấy tờ có giá; số lượng, nơi lưu giữ kim loại quý hiếm, đá quý và vật quý hiếm khác của Nhà nước; Thông tin về công nghiệp, thương mại, nông nghiệp và phát triển nông thôn; Kế hoạch vận tải có ý nghĩa quan trọng về chính trị, kinh tế - xã hội, quốc phòng, an ninh; Thông tin về quá trình xây dựng quy hoạch cấp quốc gia, quy hoạch vùng, quy hoạch tỉnh, quy hoạch đơn vị hành chính - kinh tế đặc biệt, quy hoạch đô thị, quy hoạch nông thôn; thông tin về quy hoạch hệ thống kho dự trữ quốc gia, quy hoạch hệ thống các công trình quốc phòng, khu quân sự, kho đạn dược, công nghiệp quốc phòng, an ninh.

Thông tin về tài nguyên và môi trường: tài nguyên nước, môi trường, địa chất, khoáng sản, khí tượng thủy văn, đất đai, biển, hải đảo, đo đạc và bản đồ;

Thông tin về khoa học và công nghệ: Sáng chế, công nghệ mới phục vụ quốc phòng, an ninh hoặc có ý nghĩa đặc biệt quan trọng đối với phát triển kinh tế - xã hội; Thông tin về năng lượng nguyên tử, an toàn bức xạ và hạt nhân liên quan đến quốc phòng, an ninh; Nhiệm vụ khoa học và công nghệ đặc biệt, nhiệm vụ khoa học và công nghệ cấp quốc gia liên quan đến quốc phòng, an ninh.

Thông tin về giáo dục và đào tạo: Đề thi, đáp án và thông tin liên quan đến việc tổ chức kỳ thi cấp quốc gia; Thông tin về người thuộc Quân đội nhân dân, Công an nhân dân, Cơ yếu được cử đi đào tạo trong nước và ngoài nước.

Thông tin về văn hóa, thể thao: Thông tin về di sản, di vật, cổ vật, bảo vật quốc gia; phương pháp, bí quyết sáng tạo, giữ gìn, trao truyền di sản văn hóa phi vật thể; Phương pháp, bí quyết tuyển chọn huấn luyện viên, vận động viên các môn thể thao thành tích cao; biện pháp, bí quyết phục hồi sức khỏe vận động viên sau tập luyện, thi đấu; đấu pháp trong thi đấu thể thao thành tích cao.

Lĩnh vực thông tin và truyền thông: Chiến lược, kế hoạch, đề án phát triển báo chí, xuất bản, in, phát hành, bưu chính, viễn thông và Internet, tần số vô tuyến điện, công nghệ thông tin, công nghiệp công nghệ thông tin, an toàn thông tin mạng, điện tử, phát thanh và truyền hình, thông tin điện tử, thông tấn, thông tin đối ngoại, thông tin cơ sở và hạ tầng thông tin và truyền thông quốc gia để phục vụ quốc phòng, an ninh; Thiết kế kỹ thuật, sơ đồ, số liệu về thiết bị của hệ thống thông tin quan trọng về an ninh quốc gia, hệ thống thông tin quan trọng quốc gia và hệ thống mạng thông tin dùng riêng phục vụ cơ quan, tổ chức của Đảng, Nhà nước.

Thông tin về y tế, dân số: Thông tin bảo vệ sức khỏe lãnh đạo cấp cao của Đảng, Nhà nước; Chủng, giống vi sinh vật mới phát hiện liên quan đến sức khỏe, tính mạng con người; mẫu vật, nguồn gen, vùng nuôi trồng dược liệu quý hiếm; Quy trình sản xuất dược liệu, thuốc sinh học quý hiếm; Thông tin, tài liệu, số liệu điều tra về dân số.

Thông tin về lao động, xã hội: Chiến lược, kế hoạch, đề án về cải cách tiền lương, bảo hiểm xã hội, người có công với cách mạng; Tình hình phức tạp về lao động, trẻ em, tệ nạn xã hội, bình đẳng giới.

Thông tin về tổ chức, cán bộ: Chiến lược, kế hoạch, đề án về công tác tổ chức, cán bộ của cơ quan Đảng, Nhà nước, tổ chức chính trị - xã hội; Quy trình chuẩn bị

và triển khai, thực hiện công tác tổ chức, cán bộ; Thông tin về công tác bảo vệ chính trị nội bộ; Đề thi, đáp án thi tuyển chọn lãnh đạo, quản lý và tuyển dụng, nâng ngạch công chức, viên chức.

Thông tin về thanh tra, kiểm tra, giám sát, xử lý vi phạm, giải quyết khiếu nại, tố cáo và phòng, chống tham nhũng: Chiến lược, kế hoạch, đề án về công tác thanh tra, kiểm tra, giám sát, giải quyết khiếu nại, tố cáo và phòng, chống tham nhũng; Thông tin về hoạt động thanh tra, kiểm tra, giám sát, xử lý vi phạm, giải quyết khiếu nại, tố cáo và phòng, chống tham nhũng.

Thông tin về kiểm toán nhà nước: Chiến lược, kế hoạch, đề án về kiểm toán nhà nước; Thông tin kiểm toán về tài chính công, tài sản công.

Link tham khảo: http://antoanthongtin.vn/chinh-sach---chien-luoc/quy-dinh-ve-pham-vi-bi-mat-nha-nuoc-can-duoc-bao-ve-105999

2. Cảnh báo tấn công lừa đảo dựa vào các cuộc họp Zoom giả mạo

Theo Forbes, đại dịch Covid-19 khiến tỷ lệ thất nghiệp tăng vọt. Sự không chắc chắn ở khắp mọi nơi là cơ hội để tội phạm mạng khai thác.

Điều này đã được các nhà nghiên cứu tại Sophos Labs cảnh báo sau khi phát hiện ra một chiến dịch lừa đảo mới bằng cách dụ dỗ người dùng bằng những lời mời Zoom không có thật. Những lời mời này với các chiến thuật liên quan đến cuộc họp, bảng lương… và thậm chí những từ như chấm dứt được đặt vào để tăng cường yếu tố sợ hãi.

Giống như nhiều chiến dịch tương tự, có những cảnh quan trọng, nơi người dùng nên xem rõ các email có phải là các cuộc tấn công lừa đảo và là lời mời hợp pháp hay không. Thậm chí, các email cũng tuyên bố sự hiện diện của người dùng rất quan trọng cho cuộc họp để dễ dàng đánh lừa hơn.

Khi nhận được email này, người dùng sẽ thấy các liên kết trong tin nhắn mà khi nhấp vào đó họ sẽ được đưa đến một trang web có cửa sổ đăng nhập trông giống với Zoom. Kiểm tra nhanh thanh địa chỉ của trình duyệt, người dùng sẽ thấy rằng mình không thực sự trên trang web zoom.us. Mục đích của trang web giả mạo Zoom này là đánh cắp email của người dùng.

Để tránh bị lừa, người dùng hãy nhấp vào biểu tượng ổ khóa bên cạnh địa chỉ trang web để xem thông tin về chứng chỉ SSL của nó. Trang web Zoom.us sẽ có chứng chỉ được GoDaddy cấp vào năm 2019.

Nhìn kỹ hơn vào đăng nhập giả cho thấy một chi tiết quan trọng khác, đó không chỉ là yêu cầu địa chỉ email và mật khẩu như Zoom thực sự mà yêu cầu địa chỉ email và mật khẩu email của người dùng. Theo báo cáo, những kẻ lừa đảo đằng sau các cuộc tấn công này không thực sự muốn thông tin xác thực Zoom của người dùng mà mục đích là lấy mật khẩu email. Mật khẩu email hữu ích hơn đối với kẻ tấn công - vì vậy hãy đảm bảo chỉ nhập nó trên trang web mà người dùng thực sự kiểm tra.

Khuyến nghị: Người dùng cần kiểm tra kỹ các đường link trước khi click vào, chỉ sử dụng các ứng dụng theo quy định của đơn vị khi họp trực tuyến để bảo đảm an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/canh-bao-tan-cong-lua-dao-dua-vao-cac-cuoc-hop-zoom-gia-mao-1217491.html

3. Phát hành WordPress 5.4.1 để vá nhiều lỗ hổng

Nhiều lỗ hổng nguy hiểm, phần lớn là cross-site scripting (XSS) đã được vá trong phiên bản 5.4.1 của Wordpress vừa phát hành cuối tháng tư.

WordPress 5.4.1 vá 17 lỗi và 7 lỗ hổng ảnh hưởng đến phiên bản 5.4 và trước đó. 5/7 lỗ hổng trong đó là cross-site scripting (XSS).

Một trong những lỗ hổng liên quan đến việc token đặt lại mật khẩu không được xác thực đúng cách. Cụ thể, nếu người dùng gửi yêu cầu đặt lại mật khẩu qua email, nhưng sau đó họ đăng nhập và thay đổi mật khẩu trên trang cá nhân, thì đường link đặt lại mật khẩu được gửi qua email vẫn còn hiệu lực. Tuy nhiên, để khai thác kẻ tấn công cần vào được email của nạn nhân và truy cập link đặt lại mật khẩu trong email.

Một lỗ hổng khác cho phép kẻ tấn công không xác thực xem các bài đăng riêng tư bằng cách tạo các truy vấn date/time. Tuy nhiên họ cần biết chính xác thời gian đến từng giây của bài đăng của bài đăng riêng tư.

Các lỗ hổng còn lại là cross-site scripting (XSS) trong Customizer, Search Block, wp-object-cache, và file upload. Tuy nhiên, để khai thác các lỗ hổng này cần có tài khoản đăng nhập hoặc quyền truy cập vào hệ thống, điều này có nghĩa là cần kết hợp với các lỗ hổng hoặc kiểu tấn công khác (ví dụ phishing chiếm thông tin đăng nhập và sau đó tiến hành khai thác lỗ hổng).

Các nhà phát triển cho biết block editor của Wordpress cũng ảnh hưởng bởi lỗ hổng XSS và có thể bị khai thác bởi kẻ tấn công đã được xác thực. Tuy nhiên lỗ hổng này đã được vá trong phiên bản 5.4 RC5.

Người dùng có thể tải WordPress 5.4.1 từ trang chủ tại địa chỉ WordPress.org hoặc truy cập trang quản trị Wordpress => Dashboard => Updates và bấm Update Now để cập nhật.

Nếu website sử dụng WordPress hỗ trợ tự động cập nhật, các trang này đã được cập nhật lên phiên bản 5.4.1.

Các trang web sử dụng Wordpress vẫn luôn là mục tiêu tấn công để đánh cắp dữ liệu, phát tán mã độc… do đó ngoài cập nhập các bản vá lỗi WordPress core người dùng cũng nên cập nhật bản vá cho các plugin/theme.

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

Link tham khảo: https://whitehat.vn/threads/phat-hanh-wordpress-5-4-1-de-va-nhieu-lo-hong.13566/

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	Netgear	CVE 2018 21137 CVE 2018 21132 CVE 2020 11894 ...	Nhóm 212 lỗ hổng trong các thiết bị của Netgear (WAC505, WAC510, D6000, D6100, R6800, D6620,…) cho phép đối tượng tấn công thu thập thông tin, tấn công command injection, tấn công XSS.	Đã có thông tin xác nhận và bản vá.
2	LG	CVE 2019 20777 CVE 2020 11873 CVE 2020 11873 …	Nhóm 19 lỗ hổng trong các thiết bị LG Mobile Android OS 7,8,9, cho phép đối tượng tấn công thu thập thông tin người dùng, chèn và thực thi mã từ xa, leo thang quyền.	Đã có thông tin xác nhận và bản vá
3	Google	CVE 2020 0080 CVE 2020 0081 CVE 2020 0082 …	Nhóm 16 lỗ hổng trong các phần mềm của Google (Android Android 8,9,10; Google Earth Pro versions < 7.3.3) cho phép đối tượng tấn công chèn và thực thi mã từ xa, leo thang quyền, tấn công lừa đảo.	Đã có thông tin xác nhận và bản vá
4	IBM	CVE 2019 4644 CVE 2019 4446 CVE 2020 4277 …	Nhóm 13 lỗ hổng trong phần mềm của IBM (TRIRIGA Application Platform, Cloud App Management,…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã tùy ý, tấn công giả mạo, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
5	Mozilla	CVE 2020 6826 CVE 2020 6823 CVE 2020 6824 …	Nhóm 12 lỗ hổng trong phần mềm của Mozilla (Firefox version < 75, Firefox ESR < 68.7, Thunderbird < 68.7.0) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã từ xa, tấn công phishing	Đã có thông tin xác nhận và bản vá

			URI.	
6	Wordpress	CVE 2020 11928 CVE 2020 11930 CVE 2020 12073 …	Nhóm 10 lỗ hổng trong phần mềm Wordpress (responsive add ons plugin,…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã tùy ý, tấn công XSS.	Đã có thông tin xác nhận và bản vá
7	D-link	CVE 2019 17525 CVE 2020 9275 CVE 2020 9278 …	Nhóm 06 lỗ hổng trên thiết bị D link (DSL 2640B B2 EU_4.01B, DIR 615 T1 20.10,…) cho phép đối tượng tấn công chèn và thực thi mã tùy ý, truy cập trái phép.	Chưa có thông tin xác nhận và bản vá
8	Jooomla	CVE 2020 11891 CVE 2020 11890 CVE 2020 11889	Nhóm 03 lỗ hổng trong phần mềm Joomla (Joomla! before 3.9.17) cho phép đối tượng tấn công chèn và thực thi mã tùy ý.	Chưa 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	xdqzpbcgrvkj.ru
7	track.saygggggames.io
8	xjpakmdcfuqe.in
9	xjpakmdcfuqe.ru
10	amnsreiuojy.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.