BẢN TIN NỘI BỘ

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

1. Thành lập Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam

Bộ Thông tin và Truyền thông vừa ban hành quyết định thành lập Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam trực thuộc Cục An toàn thông tin.

Theo Quyết định, việc thành lập Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam trực thuộc Cục An toàn thông tin trên cơ sở tổ chức lại Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam và Trung tâm Kiểm định an toàn thông tin.

Đây là đơn vị sự nghiệp công lập trực thuộc Cục An toàn thông tin thực hiện chức năng làm đầu mối kỹ thuật điều phối ứng cứu sự cố an toàn không gian mạng và kiểm định an toàn thông tin trên phạm vi toàn quốc; quản lý, vận hành các hệ thống số liệu, cơ sở dữ liệu, hệ thống kỹ thuật về điều phối ứng cứu sự cố, kiểm định và phòng, chống thư điện tử rác, tin nhắn rác phục vụ công tác quản lý nhà nước và thực thi pháp luật về an toàn thông tin; là đầu mối hợp tác quốc tế với các cơ quan, tổ chức có chức năng ứng cứu sự cố và kiểm định an toàn thông tin.

Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam có tên giao dịch quốc tế là Vietnam Cybersecurity mergency Response Teams/Coordination Center (VNCERT/CC), có trụ sở chính đặt tại Hà Nội và các chi nhánh tại TP. Hồ Chí Minh, Đà Nẵng.

Quyết định cũng quy định rõ các nhiệm vụ, quyền hạn của Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam, trong đó có nhiệm vụ tham gia nghiên cứu, đề xuất, xây dựng các cơ chế, chính sách, chương trình, đề án, dự án và các hướng dẫn kỹ thuật về bảo đảm an toàn thông tin theo phân công của Cục trưởng.

Điều phối các hoạt động ứng cứu sự cố an toàn thông tin trên phạm vi toàn quốc, là đầu mối của Cục An toàn thông tin để phối hợp với các cơ quan, tổ chức trong công tác ứng cứu sự cố an toàn thông tin; thực hiện kiểm định, đánh giá an toàn thông tin đối với sản phẩm phần cứng, phần mềm, hệ thống thông tin, hệ thống quản lý, vận hành an toàn thông tin mạng theo quy định của pháp luật; cấp và thu hồi giấy chứng nhận hợp chuẩn, hợp quy đối với sản phẩm phần cứng, phần mềm, hệ thống thông tin, hệ thống quản lý, vận hành an toàn thông tin mạng theo quy định của pháp luật; thực hiện đánh giá hợp chuẩn, hợp quy về an toàn thông tin mạng phục vụ hoạt động quản lý nhà nước của Cục An toàn thông tin.

Bên cạnh đó, Trung tâm cũng có các nhiệm vụ hướng dẫn, tổ chức thực hiện hoạt động diễn tập, đào tạo, tập huấn, bồi dưỡng nâng cao kiến thức, kỹ năng về an toàn thông tin cho các cơ quan, tổ chức và doanh nghiệp; tuyên truyền, phổ biến, nâng cao nhận thức và trách nhiệm về an toàn thông tin; tổ chức sự kiện, hội thảo, hội nghị về an toàn thông tin; cấp chứng nhận, chứng chỉ về an toàn thông tin, CNTT theo quy định của pháp luật…

Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam được kế thừa các quyền và nghĩa vụ hợp pháp của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam

và Trung tâm Kiểm định an toàn thông tin theo quy định. Quyết định có hiệu lực từ ngày 1/11/2019.

Link tham khảo: http://www.antoanthongtin.vn/Detail.aspx?CatID=e1999c9a-5eeb-418c-9ea8-ae4c5e850d0c&NewsID=e7586b5e-c35a-4fc4-b803-c3a3333dc2c3&MenuID=

2. Lỗ hổng nghiêm trọng cho phép truy cập trái phép điểm truy cập Aironet của Cisco

Ngày 16/10, Cisco thông báo cho khách hàng rằng một số điểm truy cập không dây Aironet (access point) của hãng bị ảnh hưởng bởi một lỗ hổng nghiêm trọng có thể bị khai thác từ xa để truy cập trái phép vào thiết bị.

Lỗ hổng, được theo dõi là CVE-2019-15260, là do việc kiểm soát truy cập vào một số URL không được thực hiện đầy đủ, cho phép kẻ tấn công giành quyền truy cập với đặc quyền nâng cao vào thiết bị bằng cách yêu cầu các URL không được bảo vệ.

"Dù kẻ tấn công không truy cập được tất cả các tùy chọn cấu hình, lỗ hổng vẫn có thể cho phép kẻ tấn công xem thông tin nhạy cảm và thay thế một số tùy chọn bằng các giá trị mà chúng chọn, bao gồm cả cấu hình mạng không dây. Lỗ hổng cũng sẽ cho phép kẻ tấn công vô hiệu hóa điểm truy cập, tạo ra điều kiện từ chối dịch vụ (DoS) trên các máy khách được liên kết với điểm truy cập", Cisco giải thích.

Lỗ hổng ảnh hưởng đến các điểm truy cập không dây Aironet 1540, 1560, 1800, 2800, 3800 và 4800. Bản vá có trong các phiên bản 8.5.151.0, 8.8.125.0 và 8.9.111.0.

Cisco cho biết chưa có bằng chứng cho thấy lỗ hổng đang bị khai thác vì mục đích xấu.

Cisco cũng tiết lộ các điểm truy cập Aironet bị ảnh hưởng bởi hai lỗ hổng có mức độ nghiêm trọng cao có thể bị khai thác mà không cần xác thực để tiến hành các cuộc tấn công từ chối dịch vụ (DoS). Một lỗ hổng ảnh hưởng đến chức năng xử lý gói VPN PPTP (Giao thức đường hầm), lỗ hổng còn lại tồn tại trong giao thức Kiểm soát và cung cấp điểm truy cập không dây (CAPWAP).

Các lỗ hổng nghiêm trọng khác được Cisco tiết lộ trong tuần này bao gồm lỗi thực thi mã từ xa trong bộ chuyển đổi điện thoại SPA100, lỗ hổng DoS trong phần mềm Bộ điều khiển mạng LAN không dây và lỗ hổng CSRF (giả mạo yêu cầu chéo) trong các thiết bị chuyển mạch thông minh và quản lý doanh nghiệp nhỏ.

Ngoại trừ SPA100, các lỗ hổng khác có thể bị khai thác từ xa mà không cần xác thực. SPA100 vẫn chưa được vá, nhưng Cisco đang tìm cách khắc phục.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng và người quản trị cần cập nhật các bản vá mới nhất của Aironet Cisco để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/lo-hong-nghiem-trong-cho-phep-truy-cap-trai-phep-diem-truy-cap-aironet-cua-cisco.12839/

3. Cảnh báo lỗ hổng thực thi lệnh từ xa không cần xác thực trên CyberoamOS

Đây là lỗ hổng cho phép kẻ tấn công truy cập vào Cyberoam - loại thiết bị tường lửa thường được sử dụng rộng rãi trong hệ thống các doanh nghiệp, tổ chức đặc biệt là trường học và ngân hàng.

Công ty cổ phần An ninh mạng Việt Nam (VSEC) đã phát đi cảnh báo về một lỗ hổng mã CVE-2019-17059 cho phép kẻ tấn công truy cập vào thiết bị Cyberoam, và thực thi lệnh trái phép từ xa mà không cần cung cấp bất kỳ tên người dùng hoặc mật khẩu.

Lỗ hổng này được phát hiện trên phiên bản CyberoamOS trước 10.6.6 MR-6 và được các chuyên gia bảo mật của VSEC đánh giá là một lỗ hổng nghiêm trọng, có thể ảnh hưởng lớn đến nhiều doanh nghiệp Việt Nam.

Để khai thác lỗ hổng này, tin tặc sẽ truy cập vào giao diện quản trị web hoặc bảng điều khiển SSL VPN (SSL VPN Consoles), sau đó gửi các gói tin chứa mã khai thác đến 2 giao diện đó để chiếm quyền điều khiển thiết bị. Nguy hiểm hơn, quyền truy cập được cấp lại là quyền cao nhất, giúp kẻ tấn công có thể làm bất kỳ hoạt động tùy ý trên thiết bị Cyberoam của bạn như tấn công sâu hơn vào hệ thống hay cài đặt backdoor, theo dõi toàn bộ dữ liệu tin nhắn, giao dịch… được truyền trong mạng.

Cyberoam là một thiết bị bảo mật dựa trên cơ sở xác thực người sử dụng, cung cấp khả năng bảo vệ trong thời gian thực đối với những dạng tấn công và mối đe dọa an ninh mạng. Theo kết quả thống kê từ Shodan (shodan.io), có hơn 96.000 thiết bị Cyberoam công khai trên internet ở khắp nơi trên thế giới. Hầu hết các thiết bị này được cài đặt trong các doanh nghiệp, trường đại học và ngân hàng nổi tiếng thế giới, giúp chống spam, virus, lọc nội dung trang web, phòng chống thâm nhập trái phép, quản lý băng thông… Vậy nếu tin tặc khai thác thành công lỗ hổng này cho các cuộc tấn công mạng, hậu quả sẽ rất khôn lường.

Để đảm bảo an toàn cho các tổ chức và doanh nghiệp Việt, VSEC khuyến cáo các đơn vị đang sử dụng tường lửa Cyberoam cần ngay lập tức cập nhật phiên bản CyberoamOS mới nhất, sử dụng các giao thức mã hóa để truyền dữ liệu kể cả trong mạng nội bộ, nâng cao năng lực, nhận thức của người dùng về an toàn bảo mật thông tin.

Khuyến nghị:

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

Link tham khảo: https://thanhnien.vn/cong-nghe/canh-bao-lo-hong-thuc-thi-lenh-tu-xa-khong-can-xac-thuc-tren-cyberoamos-1137637.html

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	Microsoft	CVE-2019-1326 CVE-2019-1327 CVE-2019-1330 …	Nhóm 60 lỗ hổng trên hệ điều hành Microsoft (Chakracore, excel, Internet Explorer, Windows 7, Windows 10…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã lệnh từ xa. 04 lỗ hổng có điểm đặc biệt nghiêm trọng là 9.3	Đã có thông tin xác nhận và bản vá.
2	Wordpress	CVE-2019-17386 CVE-2019-17385 CVE-2019-17384 …	Nhóm 32 lỗ hổng trên Wordpress cho phép đối tượng tấn công thực hiện tấn công XSS, thực thi mã lệnh tùy ý.	Chưa có thông tin xác nhận và bản vá
3	Linux	CVE-2019-17133 CVE-2019-17351	Nhóm 02 lỗ hổng trên hệ điều hành Linux (Linux kernel)cho phép đối tượng tấn công chèn và thực thi mã lệnh từ xa, tấn công từ chối dịch vụ	Đã có thông tin xác nhận và bản vá
4	Foxit software	CVE-2019-13315 CVE-2019-13316 CVE-2019-13317 …	Nhóm 10 lỗ hổng trên phần mềm Foxit Reader (Foxit Reader 9.5.0.20723, Foxit Reader 9.4.1.16828…) cho phép đối tượng tấn công chèn và thực thi mã lệnh từ xa, thu thập thông tin.	Đã có thông tin xác nhận và bản vá
5	Dlink	CVE-2019-17505 CVE-2019-17353 CVE-2019-17507 …	Nhóm 07 lỗ hổng trên thiết bị Dlink (DAP-1320 a2-v1.21, DIR-615, DIR-816 …) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã lệnh từ xa.	Chưa có thông tin xác nhận và bản vá
6	Android	CVE-2019-2183 CVE-2019-2114 CVE-2019-2186 …	Nhóm 09 lỗ hổng trên hệ điều hành Android (Android 9, Android 7.1.2, Android 10,..) cho phép đối tượng tấn công thực thi mã lệnh 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	soplifan.ru
5	ld3t8xao8.ru
6	www.cityofangelsmagazine.com
7	morphed.ru
8	xjpakmdcfuqe.com
9	xdqzpbcgrvkj.ru
10	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.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.