NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 13 (27/03/2023 – 02/04/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Cảnh báo:** Lỗ hổng bảo mật trong WordPress Elementor Pro gây ảnh hưởng đến hàng triệu website.

- **Chiến dịch tấn công APT:** Nhóm APT Winter Vivern nhằm mục tiêu vào các tổ chức Chính phủ Châu Âu thông qua lỗ hổng trên Zimbra.

2. Điểm yếu, lỗ hổng

- **926** lỗ hổng được công bố và cập nhật.

- **07** lỗ hổng, nhóm lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam.

3. Số liệu, thống kê

- **Tấn công DRDoS**

- **Tấn công Web**

- **Tấn công lừa đảo người dùng Việt Nam: 284** trường hợp lừa đảo do người dùng Internet Việt Nam thông báo.

4. Tài liệu lưu trữ

Chuyên mục **Cảnh báo tuần** tại địa chỉ:

https://service.khonggianmang.vn

https://khonggianmang.vn

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Lỗ hổng bảo mật trong WordPress Elementor Pro gây ảnh hưởng đến hàng triệu website"

Ngày 18/03/2023, một nhóm đối tượng tấn công mạng chưa được xác định danh tính đang khai thác lỗ hổng bảo mật trong plugin tạo và quản lý trang web Elementor Pro dành cho WordPress.

Các nhà nghiên cứu đã phát hiện ra lỗ hổng bảo mật trong WordPress cho phép đối tượng tấn công kiểm soát quyền truy cập, gây ảnh hưởng đến các phiên bản 3.11.6 trở về trước. Việc khai thác thành công lỗ hổng này cho phép đối tượng tấn công đã xác thực chiếm quyền kiểm soát trang web WordPress được bật WooC Commerce và thực hiện thay đổi vai trò từ người dùng mặc định thành quản trị viên nhằm lợi dụng các đặc quyền của quản trị viên.

Điều này cho phép đối tượng tấn công điều hướng trang web đến một tên miền độc hại, tải lên plugin hoặc backdoor để tiếp tục thực hiện khai thác trang web. Lỗ hổng hiện đang bị lạm dụng bởi một số địa chỉ IP nhằm mục đích tải lên các tệp lưu trữ PHP và ZIP tùy ý.

Vào ngày 22/3, WordPress đã phát hành bản vá để khắc phục lỗ hổng này, người dùng nên cập nhật Elementor Pro lên phiên bản 3.11.7 hoặc 3.12.0 nhằm giảm thiểu các mối đe dọa tiềm ẩn và đồng thời kiểm tra kỹ các trang web trước khi thực hiện truy cập.

Nguồn: https://thehackernews.com/2023/04/hackers-exploiting-wordpress-elementor.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Nhóm APT Winter Vivern nhằm mục tiêu vào các tổ chức Chính phủ Châu Âu thông qua lỗ hổng trên Zimbra"

Nhóm APT Winter Vivern hay còn gọi là TA473 (UAC-0114) đang tiến hành chiến dịch tấn công mạng nhằm mục tiêu vào các tổ chức chính phủ ở Châu Âu và Hoa kỳ.

Kể từ tháng 2/2023, Winter Vivern đã lợi dụng lỗ hổng chưa được cập nhật bản vá trong các cổng webmail trên Zimbra, lỗ hổng này cho phép đối tượng tấn công có quyền truy cập vào hộp thư email của các tổ chức Chính phủ ở Châu Âu. Ngoài ra, nhóm APT này còn liên quan đến các cuộc tấn công nhằm vào tổ chức Chính phủ các nước như Ukraine, Ba Lan, Ấn Độ, Litva, Slovakia và Vatican.

Lỗ hổng bảo mật CVE-2022-27926 có điểm CVSS: 6.1 (Trung bình), ảnh hưởng đến Zimbra Collaboration, cho phép đối tượng tấn công thực thi mã JavaScript hoặc HTML tùy ý mà không cần xác thực.

Nhóm tấn công sử dụng công cụ quét (scan) như Acunetix để xác định webmail chưa cập nhật bản vá của các tổ chức mục tiêu, sau đó gửi email lừa đảo có chứa các đường link liên kết đến những trang web độc hại.

Lỗ hổng này khai thác lỗi Cross-site scripting (XSS) trong Zimbra để thực thi các playload JavaScript độc hại trong webmail của người dùng, nhằm đánh cắp tên đăng nhập, mật khẩu và mã token để thực hiện truy cập trái phép. Điều đáng chú ý là mỗi playload đều được điều chỉnh cho phù hợp với webmail được nhằm mục tiêu, cho thấy đối tượng tấn công đã đầu tư thời gian và tài nguyên để tránh khả năng bị phát hiện.

Để đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan, tổ chức cần thực hiện kiểm tra, rà soát và cập nhật bản vá các lỗ hổng bảo mật kịp thời cho các sản phẩm công nghệ thông tin đang sử dụng. Đồng thời, sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng.

Nguồn: https://thehackernews.com/2023/03/winter-vivern-apt-targets-european.html

Nguy cơ tấn công mạng từ điểm yếu, lỗ hổng

Trong tuần, các tổ chức quốc tế đã công bố và cập nhật ít nhất 926 lỗ hổng, trong đó có 214 lỗ hổng mức Cao, 210 lỗ hổng mức Trung bình, 03 lỗ hổng mức Thấp và 499 lỗ hổng chưa đánh giá. Trong đó có ít nhất 315 lỗ hổng cho phép chèn và thực thi mã lệnh.

Hệ thống kỹ thuật của Cục ATTT chủ động rà quét trên không gian mạng Việt Nam, đánh giá, thống kê cho thấy có 07 lỗ hổng/nhóm lỗ hổng trên các sản phẩm, dịch vụ CNTT phổ biến, có thể gây ảnh hưởng lớn đến người dùng ở Việt Nam: Nhóm 158 lỗ hổng trong Google, Nhóm 20 lỗ hổng trong Linux, Nhóm 08 lỗ hổng trong Apache, Nhóm 23 lỗ hổng trong Wordpress, Nhóm 20 lỗ hổng trong Huawei, 01 lỗ hổng trong Samsung, Nhóm 24 lỗ hổng trong D-link. Thông tin chi tiết về một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam cụ thể như sau:

Một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam:

- *Google: CVE-2022-42498, CVE-2022-20532,...*
- *Linux: CVE-2023-1079, CVE-2020-36691,...*
- *Apache: CVE-2022-38745, CVE-2022-47502,...*
- *Wordpress: CVE-2020-36666, CVE-2022-47602,...*
- Huawei*: CVE-2022-48347, CVE-2022-48348,...*
- *Samsung: CVE-2022-1230.*
- *D-link: CVE-2022-43642, CVE-2022-43643,...*

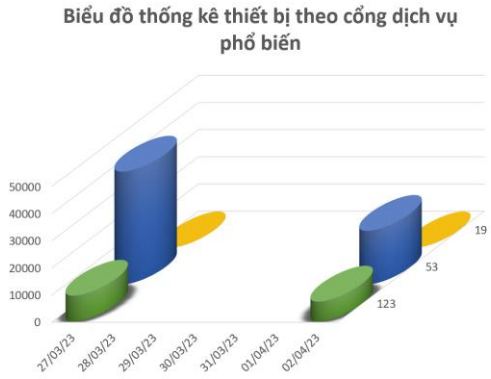
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Google	CVE-2022-20532 CVE-2022-28495 CVE-2022-42498 …	Nhóm 158 lỗ hổng trong Google (Android, Chrome,…) cho phép đối tượng tấn công thực hiện leo thang đặc quyền, thực thi lệnh tùy ý, thực thi mã từ xa, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
2	Linux	CVE-2023-1079 CVE-2020-36691 CVE-2023-1583 …	Nhóm 20 lỗ hổng trong Linux (kernel) cho phép đối tượng tấn công thực hiện tấn công thực hiện tấn công từ chối dịch vụ, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
3	Apache	CVE-2022-38745 CVE-2022-47502 CVE-2023-25197 …	Nhóm 08 lỗ hổng trong Apache cho phép đối tượng tấn công thực thi lệnh/mã tùy ý, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2020-36666 CVE-2022-47602 CVE-2022-47603 …	Nhóm 23 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực hiện tấn công XSS, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
5	Huawei	CVE-2022-48347 CVE-2022-48348 CVE-2022-48349 …	Nhóm 20 lỗ hổng trong Huawei cho phép đối tượng tấn công thực hiện leo thang đặc quyền, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
6	Samsung	CVE-2022-1230	01 lỗ hổng trong Samsung (Galaxy S21) cho phép đối tượng tấn công thực hiện leo thang đặc quyền và thực thi mã tùy ý, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
7	D-link	CVE-2022-43642 CVE-2022-43643 CVE-2022-43644 ...	Nhóm 24 lỗ hổng trong D-link (dir-825) cho phép đối tượng tấn công truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá

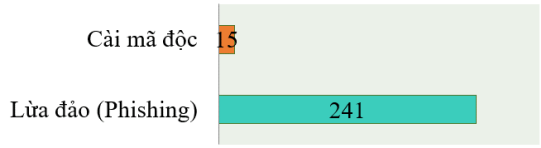
Thông kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

Tấn công DRDoS

Tuần vừa qua tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **47,608** (giảm so với tuần trước **49,098**) thiết bị có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (123), DNS (53), Chargen (19). Dưới đây là biểu đồ thống kê thiết bị theo cổng dịch vụ phổ biến trong tuần.

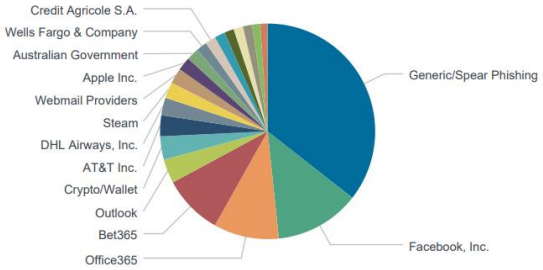


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có 256 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 241 trường hợp tấn công lừa đảo (Phishing), 15 trường hợp tấn công cài cắm mã độc.



Tấn công Phishing

Trên thế giới có nhiều các trang web giả mạo các tổ chức, doanh nghiệp, nhà cung cấp, dịch vụ lớn như: Các mạng xã hội, ngân hàng, thư điện tử,v.v…Việt Nam có nhiều người dùng các dịch vụ, ứng dụng nước ngoài (cả miễn phí và tính phí) như các mạng xã hội, Payment, Apple, Paypal,v.v… vì vậy người dùng cần phải hết sức cảnh giác với những trang web giả mạo để đánh cắp tài khoản.

Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam

differentia.ru: 18755 IP	xjpakmdcfuqe.ru:480 IP
disorderstatus.ru: 7696 IP	xjpakmdcfuqe.in:491 IP
atomictrivia.ru: 3634 IP	restlesz.su: 371 IP
xjpakmdcfuqe.biz: 746 IP	amnsreiuojy.ru: 907 IP
xjpakmdcfuqe.com: 483 IP	hzmksreiuojy.ru: 56 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có 284 phản ánh trường hợp lừa đảo do người dùng Internet Việt Nam phản ánh về Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) qua hệ thống tại địa chỉ https://canhbao.khonggianmang.vn. Qua kiểm tra, phân tích có nhiều trường hợp lừa đảo giả mạo website của ngân hàng, các trang thương mại điện tử…

Dưới đây là một số trường hợp người dùng cần nâng cao cảnh giác.

STT	Website lừa đảo	Ghi chú
1	vaymbbank.com	Website giả mạo Ngân hàng TMCP Quân đội
2	lo.dama582.com	Website giả mạo Western Union
3	shopeemallvn.com	Website giả mạo sàn TMĐT Shopee
4	vietcombank.vn-dll.vip	Website giả mạo Ngân Hàng TMCP Ngoại thương Việt Nam
5	vie-tcapital.com	Website giả mạo Ngân hàng TMCP Bản Việt
6	amazonxk.com	Website giả mạo Amazon
7	vinfast888.net phattai6666.com rik11.fun alibabavn.shop congtykiman.org vincomonevip.net trungtamthuongmaihanoi.com minhchinhmega.com mcredit.vaynhanh-bankcredits.com hackgamemienphi.com	Website giả mạo, lừa đảo

NCSC VN
National Cyber Security Center

Khuyến nghị đối với các cơ quan, đơn vị

"NỖ LỰC ĐỂ KHÔNG GIAN MẠNG VIỆT NAM LUÔN AN TOÀN, LÀNH MẠNH"

1. Đối với các nguy cơ, cảnh báo đã được đề cập trong phần **Tin tức an toàn thông tin,** Quý đơn vị cần thường xuyên cập nhật thông tin (như các chiến dịch tấn công của các nhóm APT, thông tin IoC kèm theo từng chiến dịch, điểm yếu lỗ hổng đang bị lợi dụng để khai thác,…), rà soát trên các hệ thống thông tin để phát hiện và ngăn chặn, xử lý kịp thời.

***

2. Đối với các điểm yếu, lỗ hổng trong phần **Lỗ hổng bảo mật**, Quý đơn vị cần lưu ý theo dõi và cập nhật bản vá cho các lỗ hổng liên quan đến sản phẩm đang sử dụng. Ngoài ra, những đơn vị đã có tài khoản trên "Hệ thống Cảnh báo điểm yếu và rà soát lỗ hổng bảo mật tự động" tại địa chỉ https://service.khonggianmang.vn, quản trị viên có thể thêm các sản phẩm đang sử dụng để giám sát và nhận cảnh báo ngay khi có lỗ hổng mới phát sinh.

***

3. Đối với các nguy cơ về tấn công từ chối dịch vụ, tấn công web trong phần **Thống kê nguy cơ, các cuộc tấn công tại Việt Nam**, Quý đơn vị cần rà soát, hạn chế tối đa việc mở các cổng dịch vụ có thể bị lợi dụng để thực hiện tấn công từ chối dịch vụ; thường xuyên kiểm tra, rà soát máy chủ web để kịp thời phát hiện và xử lý nguy cơ tấn công. Bên cạnh đó, đối với các IP/tên miền được đề cập trong mục **Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam**, Quý đơn vị cần kiểm tra và xử lý các thiết bị trong toàn bộ hệ thống mạng nếu có dấu hiệu kết nối đến các tên miền độc hại mà Cục ATTT đã chia sẻ.

***

4. Đối với các website giả mạo thống kê tại mục **Tấn công lừa đảo người dùng Việt Nam**, Quý đơn vị cần chú ý quan tâm không truy cập vào các trang web được nêu để tránh nguy cơ bị tấn công lừa đảo, nâng cao nhận thức bản thân và tuyên truyền cho bạn bè, người thân và những người xung quanh tránh việc trở thành nạn nhân của những cuộc tấn công lừa đảo này.

024.3209.1616
ncsc@ais.gov.vn
https://khonggianmang.vn/
https://www.facebook.com/govSOC
Tầng 16, số 115 Trần Duy Hưng, quận Cầu Giấy, Tp. Hà Nội