NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 02 (08/01/2024 – 14/01/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Lỗ hổng Zero-Day trong Ivanti VPN bị khai thác để phát tán 5 loại mã độc.

- **Cảnh báo:** Phát hiện lỗ hổng RCE nghiêm trọng trên tường lửa SRX và Switch EX của Juniper.

2. Điểm yếu, lỗ hổng

- **972** 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: 518** 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://khonggianmang.vn

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Lỗ hổng Zero-Day trong Ivanti VPN bị khai thác để phát tán 5 loại mã độc"

Trong giai đoạn hậu khai thác của hai lỗ hổng zero-day trên sản phẩm Ivanti Connect Secure (ICS) VPN từ tháng 12/2023, các chuyên gia bảo mật đã phát hiện và xác định rằng nhóm APT UNC5221 đang triển khai không dưới 5 dạng mã độc khác nhau. Các đoạn mã độc này được sử dụng nhằm phá vỡ lớp xác thực và tạo đường truy cập backdoor đến các thiết bị bị ảnh hưởng.

Chuỗi tấn công của nhóm này sử dụng hai lỗ hổng bảo mật, bao gồm: lỗ hổng bỏ qua xác thực CVE-2023-46805 và lỗ hổng chèn mã CVE-2024-21887, nhằm đạt được quyền kiểm soát đối với thiết bị. Cụ thể, hai lỗ hổng này cho phép nhóm tấn công đạt được quyền truy cập ban đầu, triển khai webshell, cài đặt backdoor trong các tập tin hợp pháp, thu thập thông tin xác thực và dữ liệu cấu hình, cũng như thâm nhập sâu hơn vào môi trường của thiết bị người dùng

Ivanti thông báo rằng chiến dịch tấn công này đã gây ảnh hưởng đến ít hơn 20 người dùng của họ và con số này có thể tăng lên do Ivanti đang sử dụng công cụ kiểm tra tính toàn vẹn để quét các thiết bị và phát hiện dấu hiệu về việc xâm nhập (IoC). Điều này chỉ ra chiến dịch có tính mục tiêu cao và đang trong quá trình đánh giá và xác minh. Bản vá an toàn thông tin cho hai lỗ hổng này được dự kiến sẽ phát hành từ ngày 22/01.

Phân tích chiến dịch tấn công cho thấy có ít nhất 5 loại mã độc khác nhau, được nhóm UNC5221 tích hợp bằng cách chèn vào các tập tin hợp pháp trong ICS và sử dụng các công cụ như BusyBox và PySoxy.

Đối với phần của thiết bị chỉ được phép đọc, nhóm đã sử dụng một script Perl có tên "sessionserver.pl" để làm cho hệ thống tệp có thể đọc/ghi, từ đó triển khai THINSPOOL. Điều này giúp ghi web shell LIGHTWIRE vào Connect Secure và thực thi các công cụ tiếp theo trong chuỗi tấn công.

LIGHTWIRE và WIREFIRE là hai webshell chủ chốt được tạo ra để đảm bảo duy trì kết nối từ xa tới các thiết bị bị ảnh hưởng. LIGHTWIRE được viết bằng ngôn ngữ Perl CGI, trong khi WIREFIRE được lập trình bằng Python.

Ngoài ra, trong chiến dịch của nhóm UNC5221 còn sử dụng mã độc đánh cắp thông tin WARPWIRE (JavaScript) và backdoor bị động ZIPLINE. ZIPLINE có khả năng thực hiện nhiều chức năng như tải lên/tải xuống file, thiết lập reverse shell, tạo máy chủ proxy, và cài đặt máy chủ tunneling để phân phối lưu lượng giữa các điểm cuối. Điều này cho thấy UNC5221 đặt mục tiêu duy trì kết nối với các mục tiêu quan trọng sau khi xâm nhập thành công.

Hiện tại, UNC5221 chưa được gán với bất kỳ nhóm APT hoặc quốc gia cụ thể nào. Tuy nhiên, thông qua phương thức tấn công tập trung vào hạ tầng vùng biên bằng việc sử dụng lỗ hổng zero-day và xâm phạm hạ tầng máy chủ C&C để tránh phát hiện bảo mật, là những đặc điểm rõ ràng của một nhóm APT.

Nguồn: https://thehackernews.com/2024/01/critical-rce-vulnerability-uncovered-in.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: SpectralBlur: Phát hiện lỗ hổng RCE nghiêm trọng trên tường lửa SRX và Switch EX của Juniper"

Juniper Networks vừa phát hành bản vá cho lỗ hổng thực thi mã từ xa (RCE) có mức độ ảnh hưởng nghiêm trọng, tồn tại trên tường lửa SRX Series và bộ chuyển đổi EX Series.

Lỗ hổng có mã định danh CVE-2024-21591 với điểm CVSS là 9.8. Lỗ hổng này cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ (DoS) hoặc thực thi mã từ xa, đồng thời đạt được quyền root trên thiết bị thông qua J-Web. Lỗ hổng CVE-2024-21591 xuất phát từ một chức năng thiếu bảo mật trên sản phẩm, cho phép đối tượng tấn công ghi đè lên bộ nhớ tùy ý.

Lỗ hổng đã được khắc phục trên các phiên bản mới, bao gồm: 20.4R3-S9, 21.2R3-S7, 21.3R3-S5, 21.4R3-S5, 22.1R3-S4, 22.2R3-S3, 22.3R3-S2, 22.4R2-S2, 22.4R3, 23.2R1-S1, 23.2R2, 23.4R1 và các phiên bản mới hơn. Đồng thời, lỗ hổng đang ảnh hưởng đến các phiên bản Junos OS dưới đây:

- Junos OS phiên bản cũ hơn 20.4R3-S9
- Junos OS 21.2 phiên bản cũ hơn 21.2R3-S7
- Junos OS 21.3 phiên bản cũ hơn 21.3R3-S5
- Junos OS 21.4 phiên bản cũ hơn 21.4R3-S5
- Junos OS 22.1 phiên bản cũ hơn 22.1R3-S4
- Junos OS 22.2 phiên bản cũ hơn 22.2R3-S3
- Junos OS 22.3 phiên bản cũ hơn 22.3R3-S2
- Junos OS 22.4 phiên bản cũ hơn 22.4R2-S2, 22.4R3

Các phiên bản ảnh hưởng đã được cập nhật, tuy nhiên, để giảm thiểu rủi ro, người dùng cần thực hiện biện pháp tạm thời như tắt J-Web hoặc hạn chế truy cập đến các máy chủ đáng tin cậy. Ngoài ra, Juniper Networks cũng đã giải quyết một lỗ hổng nghiêm trọng khác trong Junos OS và Junos OS Evolved (CVE-2024-21611, điểm CVSS: 7.5), có thể bị tấn công từ xa để gây ra tình trạng DoS.

Mặc dù không có bằng chứng về việc lỗ hổng CVE-2024-21591 đang bị khai thác nhưng nhiều lỗ hổng trước đây của SRX và EX đã bị khai thác trong năm 2023. Hơn 11.500 giao diện J-Web trên internet có thể bị các đối tượng tấn công tiếp cận, chủ yếu ở Hàn Quốc, Mỹ, Hồng Kông, Trung Quốc và Ấn Độ.

Nguồn:
https://thehackernews.com/2024/01/spectralblur-new-macos-backdoor-threat.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 **972** lỗ hổng, trong đó có 445 lỗ hổng mức Cao, 318 lỗ hổng mức Trung bình, 26 lỗ hổng mức Thấp và 183 lỗ hổng chưa đánh giá. Trong đó có ít nhất 266 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 51 lỗ hổng trong Microsoft, Nhóm 60 lỗ hổng trong Apple, Nhóm 06 lỗ hổng trong Adobe, Nhóm 87 lỗ hổng trong Wordpress, Nhóm 14 lỗ hổng trong Linux, Nhóm 24 lỗ hổng trong Tenda, Nhóm 10 lỗ hổng trong IBM. 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:

- Microsoft: CVE-2024-20672,...

- Apple: CVE-2023-42826,...

- Adobe: CVE-2024-20714, ...

- Wordpress: CVE-2023-51502,...

- Linux: CVE-2023-6040, CVE-2022-2586,...

- Tenda: CVE-2023-50585,...

- IBM: CVE-2023-47140, CVE-2023-47145,...

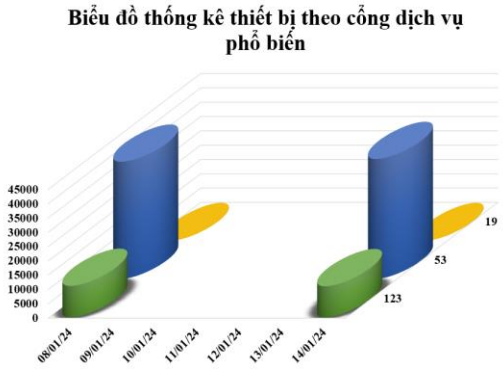
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Microsoft	CVE-2024-20672 CVE-2024-0057 CVE-2024-21312 …	Nhóm 51 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, thực thi mã từ xa, leo thang đặc quyền.	Đã có thông tin xác nhận và bản vá
2	Apple	CVE-2023-42826 CVE-2023-42876 CVE-2023-42933 …	Nhóm 60 lỗ hổng trong Apple cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, thực thi mã từ xa, leo thang đặc quyền.	Chưa có thông tin xác nhận và bản vá
3	Adobe	CVE-2024-20714 CVE-2024-20715 CVE-2024-20710 …	Nhóm 06 lỗ hổng trong Adobe cho phép đối tượng tấn công truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
4	Wordpress	CVE-2023-51502 CVE-2023-52215 CVE-2023-52218 …	Nhóm 87 lỗ hổng trong Wordpress cho phép đối tượng tấn công khai thác lỗ hổng SQL Injection, khai thác lỗ hổng CSRF, thực thi mã từ xa, thực hiện tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
5	Linux	CVE-2023-6040 CVE-2022-2586 CVE-2022-2602 …	Nhóm 14 lỗ hổng trong Linux cho phép đối tượng tấn công thực thi mã từ xa, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
6	Tenda	CVE-2023-50585 CVE-2023-49427 CVE-2023-51952 …	Nhóm 24 lỗ hổng trong Tenda cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
7	IBM	CVE-2023-47140 CVE-2023-47145 CVE-2023-31003 …	Nhóm 10 lỗ hổng trong IBM phép đối tượng tấn công leo thang đặc quyền, thực hiện tấn công từ chối dịch vụ, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá

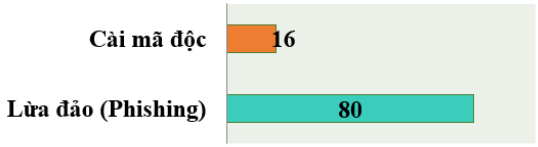
Thông kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

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 **52.856**, (tăng so với tuần trước **52.017**) 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.

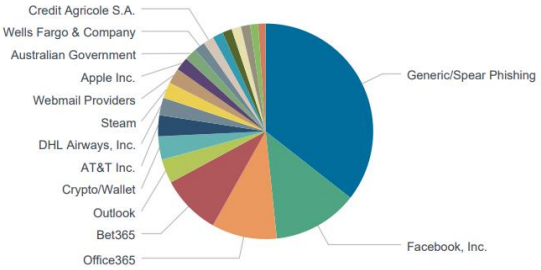


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có **96** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 80 trường hợp tấn công lừa đảo (Phishing), 16 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: 12497 IP	hzmksreiuojy.ru: 191 IP
disorderstatus.ru: 4731 IP	xjpakmdcfuqe.biz: 156 IP
atomictrivia.ru: 2242 IP	xjpakmdcfuqe.com: 47 IP
amnsreiuojy.ru: 955 IP	xjpakmdcfuqe.ru: 45 IP
restlesz.su: 294 IP	xjpakmdcfuqe.in: 47 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **518** 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	dv-ca-nhan-vpbank.com nang-cap-vip-vpbank.com dv-nang-cap-vpbank.com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
2	nanghanmucthevib.com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
3	tikivn.in dadw22.com zla963.top	Website giả mạo sàn TMĐT Tiki
4	shvnb.kfcvnpay.com	Website giả mạo Ngân hàng TMCP Sài Gòn – Hà Nội
5	vayagribank.online vayvontheoluong.site	Website giả mạo Ngân hàng nông nghiệp và phát triển nông thôn
6	shoplazada.net	Website giả mạo sàn TMĐT Lazada
7	quydautuvingroup.com vingroupinvest.com	Website giả mạo Tập đoàn Vingroup

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 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