TRUNG TÂM GIÁM SÁT AN TOÀN KHÔNG GIAN MẠNG QUỐC GIA

NCSC VN
National Cyber Security Center

CẢNH BÁO TUẦN

SỐ 31 (02/08/2021 – 08/08/2021)

Thông tin liên hệ: Trung tâm Giám sát an toàn không gian mạng quốc gia

024.3209.1616 – ais.@mic.gov.vn

Tầng 16, số 115 Trần Duy Hưng, quận Cầu Giấy, Tp.Hà Nội

NCSC VN
National Cyber Security Center

NỘI DUNG TUẦN

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

TIN CẢNH BÁO

- **Cảnh báo:** Google phát hành bản vá cho các lỗ hổng bảo mật có mức ảnh hưởng cao và nghiêm trọng trong hệ điều hành Android

- **Chiến dịch tấn công APT:** Nhóm tấn công APT DeadRinger nhằm mục tiêu đến các công ty viễn thông Đông Nam Á

ĐIỂM YẾU, LỖ HỔNG

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

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

SỐ LIỆU, THỐNG KÊ

- Tấn công DRDoS
- Tấn công Web
- Tấn công lừa đảo người dùng Việt Nam

Hot News!

Tài liệu lưu trữ:

Chuyên mục **Báo cáo định kỳ** tại địa chỉ:

https://service.khonggianmang.vn

TIN CẢNH BÁO

Cảnh báo: Google phát hành bản vá cho các lỗ hổng bảo mật có mức ảnh hưởng cao và nghiêm trọng trong hệ điều hành Android

Trong tuần vừa qua, Google đã công bố phát hành các bản cập nhật mới cho Android để xử lý vá cho hơn 30 lỗi bảo mật khiến người dùng di động phải đối mặt với hàng loạt các cuộc tấn công độc hại.

Nổi bật trong số đó là lỗ hổng bảo mật (CVE-2021-0519) trong Media framework cho phép đối tượng tấn công nâng cao đặc quyền trên thiết bị Android 8.1 và 9 hoặc thu thập thông tin trên Android 10 và 11.

Bản vá bảo mật 2021-08-01 cũng bao gồm các bản sửa lỗi cho ba lỗi đặc quyền nâng cao mức độ nghiêm trọng trong Framework và 05 lỗ hổng mức cao (02 lỗ hổng bảo mật nâng cao đặc quyền và 03 lỗ hổng đánh cắp thông tin).

Phần thứ hai của bản cập nhật bảo mật tháng này, bản vá bảo mật 2021-08-05, mang đến các bản sửa lỗi cho tổng số 24 lỗ hổng ảnh hưởng đến các thành phần Kernel, thành phần MediaTek, Widevine DRM, các thành phần Qualcomm và các thành phần nguồn đóng Qualcomm. Các lỗ hổng này cho phép kẻ tấn công thực thi mã tùy ý với các đặc quyền của Kernel.

Ngoài các lỗ hổng bảo mật đã được giải quyết bằng Bản tin bảo mật Android tháng 8 năm 2021 vừa qua, Google cũng đã sửa ba lỗi ở mức độ trung bình dành riêng cho các thiết bị của Google bằng cách nâng cao đặc quyền trong thành phần Pixel và hai lỗ hổng không xác định khác trong các thành phần nguồn đóng của Qualcomm. Tất cả các vấn đề này đã được khắc phục trên các thiết bị Pixel chạy cấp bản vá 2021-08-05.

Nguồn: https://www.securityweek.com/google-patches-high-risk-android-security-flaws?&web_view=true

Nhóm tấn công APT DeadRinger nhằm mục tiêu đến các công ty viễn thông Đông Nam Á

Gầy đây, 3 chiến dịch gián điệp mạng đã được phát hiện, theo các nhà nghiên cứu bảo mật, đối tượng tấn công đã xâm nhập các nhà cung cấp tập trung để nhằm mục tiêu vào mạng lưới các công ty viễn thông lớn tại các nước Đông Nam Á.

Mục tiêu của các chiến dịch tấn công này là nhằm vào các công ty viễn thông để tại điều kiện cho hoạt động gián điệp mạng bằng cách thu thập thông tin quan trọng và sau đó nhằm vào các tài sản lớn của các công ty.

3 chiến dịch được phát hiện:

Nhóm đầu tiên có khả năng thực hiện bởi nhóm APT Soft Cell, cuộc tấn công bắt đầu vào năm 2018. Nhóm này đã có hoạt động từ năm 2012.

Cuộc tấn công thứ 2 được cho là liên quan đến nhóm Naikon đã nhằm vào các công ty viễn thông từ Quý IV/2020.

Chiến dịch tấn công thứ 3 được liên kết với nhóm APT27 (hay còn gọi là Emissary Panda) với các hoạt động được phát hiện từ năm 2017 đến Quý I/2021. Nhóm này được phát hiện sử dụng 1 cửa hậu duy nhất để nhằm mục tiêu các máy chủ Microsoft Exchange.

Nguồn: https://cyware.com/news/deadringer-apt-group-targets-southeast-asian-telecommunications-firms-5d0b0e8e

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 531 lỗ hổng, trong đó có 21 lỗ hổng mức cao, 61 lỗ hổng mức trung bình, 15 lỗ hổng mức thấp và 434 lỗ hổng chưa đánh giá. Trong đó có ít nhất 79 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 08 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 46 lỗ hổng trong các Wordpress Plugin, Nhóm 31 lỗ hổng trong phần mềm Google, Nhóm 27 lỗ hổng trong sản phẩm của Huawei, Nhóm 26 lỗ hổng trong phần mềm Foxit, Nhóm 20 lỗ hổng trong phần mềm Liferay, Nhóm 16 lỗ hổng trong các sản phẩm Fortinet, Nhóm 11 lỗ hổng trong các sản phẩm IBM, Nhóm 10 lỗ hổng trong các sản phẩm của Dell. 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:

- Wordpress: CVE-2021-24498, CVE-2021-24479,...

- Google: CVE-2021-30566, CVE-2021-30573,...

- Huawei: CVE-2021-22444, CVE-2021-22387,...

- Foxit: CVE-2021-34843, CVE-2021-34853,...

- Liferay: CVE-2021-33335, CVE-2021-33320,...

- Fortinet: CVE-2021-36168, CVE-2021-32597,...

- IBM: CVE-2021-29741, CVE-2021-29781,...

- Dell: CVE-2021-21576, CVE-2021-21581

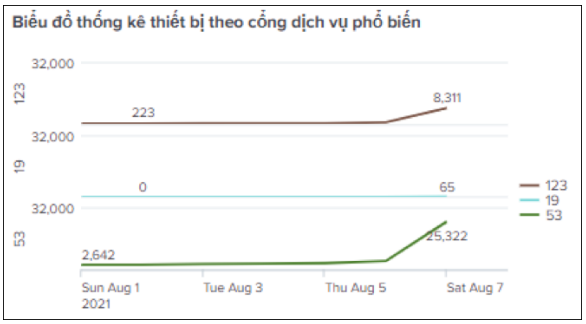
Thông tin điểm yếu, lỗ hổng

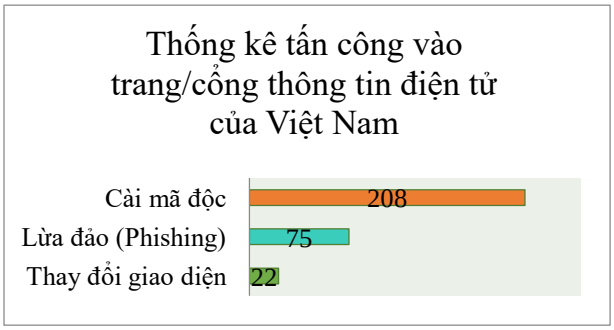
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Wordpress	CVE-2021-24498 CVE-2021-24479 CVE-2021-24371 …	Nhóm 46 lỗ hổng trong các Wordpress Plugin cho phép đối tượng tấn công thực hiện tấn công XSS, SSRF, SQL Injection, Remote File Inclusion, CSRF.	Đã có thông tin xác nhận và bản vá
2	Google	CVE-2021-30566 CVE-2021-30573 CVE-2021-30575 …	Nhóm 31 lỗ hổng trong phần mềm Google (Chrome) cho phép đối tượng tấn công thu thập thông tin, leo thang quyền, tấn công giả mạo tên miền.	Đã có thông tin xác nhận và bản vá
3	Huawei	CVE-2021-22444 CVE-2021-22387 CVE-2021-22388 …	Nhóm 27 lỗ hổng trong sản phẩm của Huawei (Huawei Smartphone) cho phép đối tượng tấn công thực thi mã từ xa, leo thang đặc quyền, tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
4	Foxit	CVE-2021-34843 CVE-2021-34853 CVE-2021-34852 …	Nhóm 26 lỗ hổng trong phần mềm Foxit (Foxit PDF Reader) cho phép đối tượng tấn công thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá
5	Liferay	CVE-2021-33335 CVE-2021-33320 CVE-2021-33333 …	Nhóm 20 lỗ hổng trong phần mềm Liferay (Liferay Portal, Liferay DXP) cho phép đối tượng tấn công thu thập thông tin, leo thang đặc quyền, gửi email spam, truy cập trái phép, tấn công XSS, CSRF.	Đã có thông tin xác nhận và bản vá
6	Fortinet	CVE-2021-36168 CVE-2021-32597 CVE-2021-32587 …	Nhóm 16 lỗ hổng trong các sản phẩm Fortinet (FortiPortal , FortiManager) cho phép đối tượng tấn công thu thập thông tin, tấn công XSS, SSRF, CRLF, SQL Injection, truy cập trái phép, thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá
7	IBM	CVE-2021-29741 CVE-2021-29781 CVE-2021-20539 …	Nhóm 11 lỗ hổng trong các sản phẩm IBM (Cloud Pak for Security,…) cho phép đối tượng tấn công thu thập thông tin, tấn công CSRF, leo thang đặc quyền, thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá
8	Dell	CVE-2021-21576 CVE-2021-21581 CVE-2021-21580 …	Nhóm 10 lỗ hổng trong các sản phẩm của Dell (EMC iDRAC9,…) cho phép đối tượng tấn công thực hiện tấn công XSS, tấn công open redirect, tấn công từ chối dịch vụ, leo thang đặc quyền.	Đã có thông tin xác nhận và bản vá

Thống kê nguy cơ, các cuộc tấn công tại 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 **55,224** (tăng so với tuần trước **51,069**) 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.



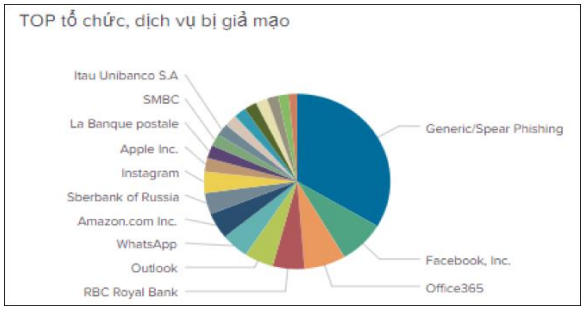


Tấn công Phishing

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 có phí) như các mạng xã hội, Paypment, Apple, Paypal ..v.v… vì vậy người dùng cần phải hết sức cảnh giác với những trang web giả mạo để ăn trộm tài khoản.

Tấn công Web

Trong tuần, có 305 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 22 trường hợp tấn công thay đổi giao diện, 75 trường hợp tấn công lừa đảo (Phishing), 208 trường hợp tấn công cài cắm mã độc.



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

differentia.ru	a.asense.in
disorderstatus.ru	ww2.bbbjdnxbgp3.ru
atomictrivia.ru	a.deltaheavy.ru
morphed.ru	sdk.asense.in
ydbnsrt.me	soplifan.ru

New

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có 52 phản ánh trường hợp lừa đảo do người dùng Internet Việt Nam thông báo 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 như lừa đảo giả mạo website của ngân hàng, lừa đảo liên quan đến COVID…..

Dưới đây một số trường hợp điển hình người dùng cần nâng cao cảnh giác trong các trường hợp tương tự.

STT	Website lừa đảo	Ghi chú
1	http://gradeup.moonfruit.com/	Website giả mạo Zimbra
2	https://www.emailmeform.com/builder/form/f5eYgf8C8eWB5zVacv9xad1L	Giả mạo cập nhật tài khoản email
3	http://dichvumxh247.com/	Lừa đảo cung cấp dịch vụ tăng người theo dõi facebook
4	https://vikin.org.vn/	Lừa đảo mua hàng trực tuyến
5	https://7879898.com/	Thu hút người dùng nạp tiền vào tài khoản để đặt mua hàng trên sàn ảo
6	www.ibidv.vip Http://www.ebidv.vip	Giả mạo website ngân hàng BIDV
7	https://home.766876.com/agentid/892265	Lừa đảo đăng ký tài khoản để kiếm tiền
8	dichvunhantien24h.cf	Giả mạo WesternUnion
9	ebankingshopee.vn https://ibankingshopee.vn/	Lừa đảo tài khoản ngân hàng thông qua tin nhắn trên app shopee
10	h5.766876.com	Lừa đảo nạp tiền
11	https://www.foreovietnam.me/foreo-sale	Giả mạo website bán hàng của Foreo

Khuyến nghị đối với các cơ quan, đơn vị

1. Đối với các nguy cơ, cảnh báo đã được đề cập trong phần **Tin cảnh báo** 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 **Nguy cơ tấn công mạng từ điểm yếu lỗ hổng**, 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.

***

4. 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.

***

Thông tin liên hệ:

Trung tâm Giám sát an toàn không gian mạng quốc gia

024.3209.1616 - ais@mic.gov.vn