NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 04 (22/01/2024 – 28/01/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Microsoft đưa ra cảnh báo về việc mở rộng phạm vi tấn công lừa đảo lên các tổ chức toàn cầu của nhóm APT29.

- **Cảnh báo:** Lỗ hổng nghiêm trọng khiến máy chủ Jenkins đối mặt với nguy cơ bị tấn công thực thi mã từ xa.

2. Điểm yếu, lỗ hổng

- **616** 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: 281** 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: Microsoft đưa ra cảnh báo về việc mở rộng phạm vi tấn công lừa đảo lên các tổ chức toàn cầu của nhóm APT29"

Trong tuần qua, Microsoft đã thông báo rằng nhóm tấn công APT29, được cho là được hậu thuẫn bởi chính phủ Nga, sau chiến dịch tấn công vào hệ thống của Microsoft vào tháng 11/2023, hiện đang mở rộng hoạt động của mình để nhắm tới nhiều tổ chức trên khắp thế giới. Microsoft đang triển khai thông báo chính thức đến các tổ chức bị ảnh hưởng, điều này được thực hiện ngay sau khi Hewlett Packard Enterprise (HPE) công bố rằng họ đã là nạn nhân của một cuộc tấn công thực hiện bởi nhóm APT29, còn được biết đến với các tên gọi khác như BlueBravo, Cloaked Ursa, Cozy Bear, Midnight Blizzard và The Dukes.

Nhóm APT29 chủ yếu tập trung vào các tổ chức chính phủ, ngoại giao, tổ chức phi chính phủ và nhà cung cấp dịch vụ IT, đặc biệt tại Mỹ và Châu u. Mục tiêu hàng đầu của nhóm trong các chiến dịch là thu thập thông tin chiến lược quan trọng với lợi ích cho Nga thông qua việc duy trì kết nối trong thời gian dài mà không gây sự chú ý.

Theo thông tin mới nhất được công bố, quy mô của chiến dịch lần này lớn hơn so với ước tính ban đầu, tuy nhiên Microsoft không tiết lộ danh sách các tổ chức bị ảnh hưởng. Nhóm APT29 thực hiện hoạt động của mình bằng cách sử dụng các tài khoản chính thức trước đó bị chiếm dụng để truy cập và mở rộng quyền kiểm soát trong môi trường tổ chức, nhằm tránh bị phát hiện. Ngoài ra, nhóm tấn công còn xác định và khai thác ứng dụng OAuth để di chuyển trong hạ tầng cloud và thực hiện các hành vi hậu khai thác như thu thập email.

Điểm mạnh trong chiến thuật tấn công của nhóm APT29 là sử dụng tài khoản người dùng đã bị xâm nhập để tạo, chỉnh sửa, và cấp quyền cao hơn cho ứng dụng OAuth. Điều này giúp nhóm APT29 duy trì kết nối với ứng dụng ngay cả khi mất quyền truy cập vào tài khoản ban đầu. Cuối cùng, ứng dụng OAuth độc hại được sử dụng để xác thực vào Microsoft Exchange Online và tấn công tài khoản email doanh nghiệp của Microsoft để thu thập thông tin.

Trong cuộc tấn công vào Microsoft tháng 11/2023, nhóm APT29 đã dùng kỹ thuật password spray (kỹ thuật chỉ sử dụng một mật khẩu phổ biến để dò đoán cho tất cả tài khoản tồn tại trong hệ thống) để xâm nhập vào một tài khoản kiểm thử không có xác thực hai yếu tố. Sau đó, chúng sử dụng tài khoản này để xác định và xâm nhập vào một ứng dụng Oauth thử nghiệm có đặc quyền cao trong môi trường doanh nghiệp Microsoft và cấp cho nó quyền full_access_as_app trong Office 365 Exchange Online để truy cập hộp thư.

Cuộc tấn công được thực hiện từ một hạ tầng proxy dân cư phân tán nhằm ẩn danh, cho phép kẻ tấn công thực hiện các thao tác với tài khoản và ứng dụng Exchange Online thông qua dải địa IP được sử dụng bởi nhiều người dùng hợp pháp khác.

Nguồn: https://thehackernews.com/2024/01/microsoft-warns-of-widening-apt29.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: SpectralBlur: Lỗ hổng nghiêm trọng khiến máy chủ Jenkins đối mặt với nguy cơ bị tấn công thực thi mã từ xa."

Jenkins là một phần mềm mã nguồn mở được sử dụng để tự động hóa quá trình liên tục tích hợp (CI), liên tục triển khai (CD) và triển khai mã nguồn (deployment). Nhóm phát triển Jenkins vừa công bố bản vá cho 9 lỗ hổng bảo mật, trong đó có một lỗ hổng nghiêm trọng (CVE-2024-23897) cho phép đối tượng tấn công thực thi mã từ xa nếu bị khai thác.

Lỗ hổng CVE-2024-23897 cho phép đối tượng tấn công đọc bất kỳ file nào thông qua giao diện dòng lệnh tích hợp (CLI). Nguyên nhân của vấn đề này là do Jenkins sử dụng một thư viện gọi là args4j để xử lý các đối số và tùy chọn khi thực hiện các lệnh CLI trên bộ điều khiển Jenkins. Trong quá trình này, trình phân tích lệnh có chức năng thay thế ký tự "@" đứng trước đường dẫn file trong đối số bằng nội dung của file (expandAtFiles). Đây là một tính năng mặc định và chỉ áp dụng cho các phiên bản cũ hơn Jenkins 2.411 và LTS 2.426.2 trở về trước.

Đối tượng tấn công sử dụng lỗ hổng để đọc các file trong hệ thống Jenkins bằng cách sử dụng mã hóa ký tự mặc định. Nếu có quyền "Overall/Read", các đối tượng này có thể đọc toàn bộ tệp, trong khi không có quyền này thì chỉ đọc được ba dòng đầu tiên tùy thuộc vào lệnh CLI. Ngoài ra, lỗ hổng CVE-2024-23897 cũng có thể bị khai thác để đọc tệp nhị phân chứa khóa mã hóa, nhưng với những hạn chế do chức năng bị ảnh hưởng đọc tệp như chuỗi sử dụng mã hóa ký tự mặc định của tiến trình điều khiển.

Trong trường hợp nội dung mật từ các tệp nhị phân bị trích xuất, Jenkins cảnh báo về nguy cơ tấn công bằng nhiều hình thức khác nhau, bao gồm:

- Thực thi mã từ xa qua Resource Root URL.
- Thực thi mã từ xa thông qua cookie "Remember me".
- Thực thi mã từ xa bằng cách tấn công XSS qua nhật ký xây dựng.
- Thực thi mã từ xa thông qua việc bypass bảo mật CSRF.
- Giải mã các nội dung mật lưu trong Jenkins.
- Xóa bất kỳ mục nào trong Jenkins.
- Tải xuống bản chụp heap Java.

Hiện nay, lỗ hổng CVE-2024-23897 đã được khắc phục trong Jenkins 2.442 và LTS 2.426.3 bằng cách vô hiệu hóa chức năng phân tích câu lệnh. Trước khi cập nhật bản vá, người dùng nên tắt truy cập tới CLI. Thông tin này được công bố gần một năm sau khi Jenkins thông báo về hai lỗ hổng bảo mật nghiêm trọng có tên là CorePlague (CVE-2023-27898 và CVE-2023-27905), cho phép kẻ tấn công thực hiện mã từ xa trên các hệ thống bị ảnh hưởng.

Nguồn: https://thehackernews.com/2024/01/critical-jenkins-vulnerability-exposes.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 **616** lỗ hổng, trong đó có 170 lỗ hổng mức Cao, 211 lỗ hổng mức Trung bình, 16 lỗ hổng mức Thấp và 219 lỗ hổng chưa đánh giá. Trong đó có ít nhất 145 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 13 lỗ hổng trong Linux, Nhóm 11 lỗ hổng trong Google, Nhóm 25 lỗ hổng trong Apple, Nhóm 17 lỗ hổng trong Wordpress, Nhóm 05 lỗ hổng trong Gitlab, Nhóm 06 lỗ hổng trong Microsoft, Nhóm 14 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:

- Linux: CVE-2023-6531, CVE-2024-0775,...

- Google: CVE-2024-0804, CVE-2024-0805,...

- Apple: CVE-2024-23203, CVE-2024-23204,...

- Wordpress: CVE-2022-40700, CVE-2023-7063,...

- Gitlab: CVE-2024-0402, CVE-2023-5933,...

- Microsoft: CVE-2024-21326, CVE-2024-21385,...

- IBM: CVE-2023-45193, CVE-2023-47152,...

Thông tin điểm yếu, lỗ hổng

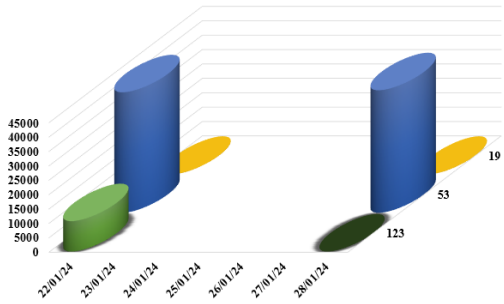
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Linux	CVE-2023-6531 CVE-2024-0775 CVE-2024-22099 …	Nhóm 13 lỗ hổng trong Linux cho phép đối tượng tấn công truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
2	Google	CVE-2024-0804 CVE-2024-0805 CVE-2024-0806 …	Nhóm 11 lỗ hổng trong Google 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
3	Apple	CVE-2024-23203 CVE-2024-23204 CVE-2024-23209 …	Nhóm 25 lỗ hổng trong Apple cho phép đối tượng tấn công thực thi mã từ xa, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2022-40700 CVE-2023-7063 CVE-2023-6290 …	Nhóm 17 lỗ hổng trong Wordpress cho phép đối tượng tấn công khai thác lỗ hổng SSRF, khai thác lỗ hổng XSS, thực thi mã từ xa, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
5	Gitlab	CVE-2024-0402 CVE-2023-5933 CVE-2023-6159 …	Nhóm 05 lỗ hổng trong Gitlab 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
6	Microsoft	CVE-2024-21326 CVE-2024-21385 CVE-2024-21387 …	Nhóm 06 lỗ hổng trong Microsoft cho phép đối tượng tấn công leo thang đặc quyền, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
7	IBM	CVE-2023-45193 CVE-2023-47152 CVE-2023-47718 …	Nhóm 14 lỗ hổng trong IBM phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, khai thác lỗ hổng CSRF, khai thác lỗ hổng SSRF, thực hiện tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá

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

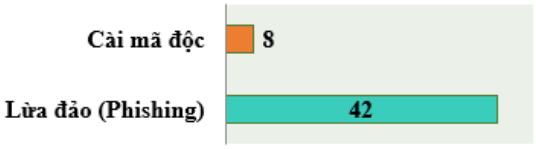
Tấn công DRDoS

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 **53.422**, (tăng so với tuần trước **52.500**) 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.

Biểu đồ thống kê thiết bị theo cổng dịch vụ phổ biến

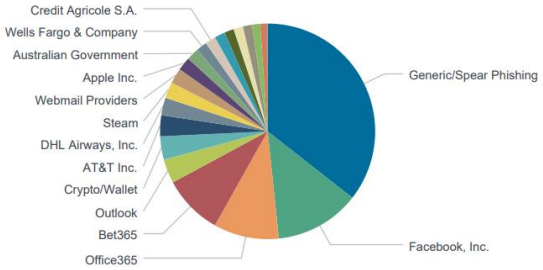


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có **50** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 42 trường hợp tấn công lừa đảo (Phishing), 08 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: 20246 IP	hzmksreiuojy.ru: 285 IP
disorderstatus.ru: 9840 IP	xjpakmdcfuqe.biz: 478 IP
atomictrivia.ru: 4724 IP	xjpakmdcfuqe.com: 349 IP
amnsreiuojy.ru: 1451 IP	xjpakmdcfuqe.ru: 304 IP
restlesz.su: 278 IP	xjpakmdcfuqe.in: 266 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **281** 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	aeshopvn.com	Website giả mạo Công ty TNHH Aeon Việt Nam
2	ssvnshop.com	Website giả mạo sàn TMĐT Shopee
3	tiki98.com	Website giả mạo sàn TMĐT Tiki
4	vingroup.fit	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