NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 35 (26/08/2024 – 01/09/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT Volt Typhoon từ Trung Quốc khai thác lỗ hổng zero-day trên Versa Director nhằm tấn công lĩnh vực IT ở Mỹ và trên toàn cầu.

- **Cảnh báo:** Lỗ hổng nghiêm trọng trên plugin WPML khiến website WordPress đối mặt với lỗi thực thi mã từ xa.

2. Điểm yếu, lỗ hổng

- TOP **10** lỗ hổng đáng chú ý trong tuần.

3. Số liệu, thống kê

- **Tấn công DRDoS**

- **Tấn công Web**

- **Botnet ảnh hưởng tới người dùng Việt Nam**

- **Tấn công lừa đảo người dùng Việt Nam: 774** 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

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT Volt Typhoon từ Trung Quốc khai thác lỗ hổng zero-day trên Versa Director nhằm tấn công lĩnh vực IT ở Mỹ và trên toàn cầu"

Mới đây, các chuyên gia bảo mật đã ghi nhận một chiến dịch tấn công do nhóm Volt Typhoon thực hiện, khai thác một lỗ hổng zero-day trên Versa Director. Mục tiêu của chiến dịch là triển khai webshell độc hại nhằm đánh cắp dữ liệu và xâm nhập vào hệ thống mạng của các doanh nghiệp thuộc các lĩnh vực cung cấp dịch vụ Internet (ISP), nhà cung cấp dịch vụ quản lý (MSP) và công nghệ thông tin (IT), gây ảnh hưởng đến bốn tổ chức tại Mỹ và một tổ chức quốc tế khác từ ngày 12/06/2024.

Lỗ hổng có mã định danh CVE-2024-39717 (điểm CVSS: 6.6), là một lỗi tải lên tệp tin trong Versa Director, cho phép đối tượng tấn công có quyền quản trị viên tải lên các tệp tin độc hại được ngụy trang dưới dạng tệp .PNG thông qua tùy chọn "Change Favicon" trong giao diện của Versa Director.

Chuỗi tấn công của chiến dịch này nổi bật với việc khai thác lỗ hổng để triển khai một webshell độc hại có tên VersaMem (tên tệp "VersaTest.png"), được thiết kế nhằm giám sát và thu thập thông tin xác thực trong các gói tin, cho phép đối tượng tấn công truy cập vào mạng của các khách hàng dưới danh nghĩa người dùng hợp lệ, gây ra một cuộc tấn công vào chuỗi cung ứng. Một điểm nổi bật khác của webshell này là tính năng module, cho phép Volt Typhoon nạp thêm mã Java để thực thi trực tiếp trong bộ nhớ.

Mẫu VersaMem đầu tiên đã được tải lên VirusTotal vào ngày 07/06/2024 và cho đến ngày 27/08/2024, chưa có giải pháp chống mã độc nào nhận diện được web shell này là độc hại. Các chuyên gia bảo mật tin rằng đối tượng tấn công đã thử nghiệm web shell này trên các hệ thống của những tổ chức quốc tế trước khi chính thức triển khai tấn công vào Mỹ.

Cụ thể, web shell này sử dụng Java instrumentation và Javassist để chèn mã độc vào bộ nhớ của tiến trình máy chủ web Tomcat trên các máy chủ Versa Director đã bị xâm nhập.

Nguồn: https://thehackernews.com/2024/08/chinese-volt-typhoon-exploits-versa.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT Volt Typhoon từ Trung Quốc khai thác lỗ hổng zero-day trên Versa Director nhằm tấn công lĩnh vực IT ở Mỹ và trên toàn cầu"

Sau khi chèn mã độc thành công, nó sẽ tích hợp vào chức năng xác thực của Versa, cho phép đối tượng tấn công thu thập thông tin xác thực dưới dạng văn bản không qua mã hóa, gây ra các cuộc tấn công vào chuỗi cung ứng. Ngoài ra, web shell còn tích hợp với chức năng lọc yêu cầu của Tomcat, cho phép đối tượng tấn công thực thi mã Java trực tiếp trong bộ nhớ, đồng thời tránh được các phương pháp phát hiện dựa trên tệp tin, bảo vệ web shell, các module và lỗ hổng zero-day mà nó khai thác.

Các chuyên gia bảo mật khuyến nghị nếu người dùng chưa thể cập nhật bản vá thì nên chặn truy cập tới các cổng 4566 và 4570, rà quét các tệp .PNG và lưu lượng mạng từ thiết bị mạng đến cổng 4566 trên các máy chủ Versa Director.

Thông tin về nhóm Volt Typhoon (còn được biết đến với các tên gọi khác như Bronze Silhouette, Insidious Taurus, UNC3236, Vanguard Panda, và Voltzite) cho thấy đây là một nhóm đối tượng tấn công đã hoạt động ít nhất năm năm, chủ yếu nhắm vào các cơ sở hạ tầng quan trọng tại Mỹ và Guam với mục tiêu duy trì kết nối ẩn và đánh cắp dữ liệu nhạy cảm.

Tuy nhiên, Trung tâm Ứng phó Khẩn cấp Virus Máy tính Quốc gia Trung Quốc (CVERC) đã phủ nhận cáo buộc này, cho rằng Volt Typhoon thực chất là một nhóm ransomware có tên Dark Power và là sản phẩm của các cơ quan tình báo Hoa Kỳ nhằm bôi nhọ Trung Quốc.

Một số IoC được ghi nhận:

VersaTest.png (VersaMem web shell)
4bcedac20a75e8f8833f4725adfc87577c32990c3783bf6c743f14599a176c37

Nguồn: https://thehackernews.com/2024/08/chinese-volt-typhoon-exploits-versa.html

Tin tức An toàn thông tin

"Cảnh báo: Lỗ hổng nghiêm trọng trên plugin WPML khiến website WordPress đối mặt với lỗi thực thi mã từ xa"

Một lỗ hổng bảo mật nghiêm trọng đã được phát hiện trên plugin WPML của WordPress, cho phép các đối tượng tấn công có quyền người dùng xác thực thực thi mã từ xa tùy ý. Lỗ hổng này có mã CVE-2024-6386 (Điểm CVSS: 9.9), ảnh hưởng đến tất cả các phiên bản của plugin trước phiên bản 4.6.13. Nguyên nhân là do thiếu sót trong việc kiểm tra và xử lý sạch dữ liệu đầu vào.

WPML là một plugin phổ biến cho việc tạo các trang web WordPress đa ngôn ngữ, hiện có hơn 1 triệu lượt cài đặt.

Chi tiết lỗ hổng do một chuyên gia bảo mật cung cấp cho thấy vấn đề xảy ra khi plugin xử lý các shortcode để hiển thị nội dung như âm thanh, hình ảnh, và video. Plugin này sử dụng mẫu Twig để tạo nội dung từ shortcode nhưng không kiểm tra và xử lý dữ liệu đầu vào đúng cách, dẫn đến lỗi server-side template injection (SSTI). Lỗi SSTI cho phép đối tượng tấn công chèn mã độc vào các mẫu hiển thị của ứng dụng, khiến mã độc được thực thi trên máy chủ.

Đối tượng tấn công có thể khai thác lỗi này để thực thi mã tùy ý và chiếm quyền kiểm soát website.

Nhà phát triển plugin đã phát hành bản vá để khắc phục lỗ hổng này. Họ cũng cho biết, lỗ hổng khó bị khai thác trong thực tế vì nó yêu cầu tài khoản bị chiếm dụng phải có quyền chỉnh sửa nội dung trong WordPress và trang web cần có cấu hình đặc biệt. Tuy nhiên, người dùng vẫn nên cập nhật bản vá càng sớm càng tốt để giảm thiểu rủi ro.

Hiện tại, nhà phát triển plugin đã phát hành bản vá để khắc phục lỗ hổng này. Mặc dù các nhà phát triển cho rằng lỗ hổng khó có thể bị khai thác trong thực tế do yêu cầu tài khoản người dùng bị chiếm đoạt phải có quyền chỉnh sửa nội dung trên WordPress và website phải có cấu hình đặc biệt. Tuy nhiên, người dùng vẫn nên cập nhật bản vá sớm nhất có thể để giảm thiểu rủi ro và bảo vệ hệ thống khỏi các mối đe dọa tiềm ẩn.

Nguồn: https://thehackernews.com/2024/08/critical-wpml-plugin-flaw-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 **630** lỗ hổng, trong đó có 266 lỗ hổng mức Cao, 185 lỗ hổng mức Trung bình, 13 lỗ hổng mức Thấp và 166 lỗ hổng chưa đánh giá. Trong đó có ít nhất 118 lỗ hổng cho phép chèn và thực thi mã lệnh.

Ngoài ra, tuần hệ thống kỹ thuật của NCSC cũng đã ghi nhận TOP **10** lỗ hổng đáng chú ý, là những lỗ hổng có mức độ nghiêm

Trong đó, đáng chú ý có **03** lỗ hổng ảnh hưởng các sản phẩm của GitHub, Google và Jenkins, cụ thể là như sau:

- **CVE-2024-6800 (Điểm CVSS: N/A):** Lỗ hổng là lỗi "XML signature wrapping" tồn tại trên GitHub Enterprise Server (GHES) cho phép đối tượng tấn công có thể sử dụng làm giả một phản hồi SAML để leo thang đặc quyền đạt được quyền quản trị ứng dụng. Hiện lỗ hổng chưa có mã khai thác và chưa có ghi nhận bị khai thác bởi các đối tượng tấn công trong thực tế.
- **CVE-2024-7965 (Điểm CVSS: 8.8 – Cao):** Lỗ hổng tồn tại trên Google Chrome cho phép đối tượng tấn công khai thác lỗi Heap Corruption sử dụng một trang HTML độc hại, qua đó truy cập và thực thi các hành vi trái phép trên hệ thống. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác bởi các đối tượng tấn công trong thực tế.
- **CVE-2024-23897 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên Jenkins cho phép đối tượng tấn công khai thác chức năng trong parser lệnh CLI để truy cập và đọc các file tùy ý tỏng file system của bộ điều khiển Jenkins. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế bởi các đối tượng tấn công.

TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	CVE-2024-6800	- Điểm CVSS: N/A - Ảnh hưởng: GitHub Enterprise Server - Mô tả: Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền, truy cập và thực thi các hành vi trái phép. - Lỗ hổng chưa có mã khai thác và chưa bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-6800
2	CVE-2024-7965	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Google Chrome - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-7965
3	CVE-2024-23897	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Jenkins - Mô tả: Lỗ hổng cho phép đối tương tấn công truy cập và thực thi các hành vi trái phép. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-23897
4	CVE-2024-43044	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Jenkins - Mô tả: Lỗ hổng cho phép đối tương tấn công thực thi mã từ xa, truy cập và thực thi các hành vi trái phép. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-43044
5	CVE-2024-5274	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Google Chrome - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-5274

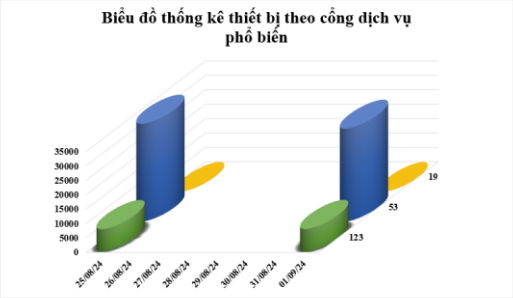
TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-38080	- Điểm CVSS: 7.8 (Trung bình) - Ảnh hưởng: Microsoft Windows Server 2022, Windows 11. - Mô tả: Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền trên hệ thống. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-38080
7	CVE-2024-5932	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Plugin GiveWP của WordPress. - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-5932
8	CVE-2024-0195	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: spider-flow - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Lỗ hổng chưa có mã khai thác và chưa bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-0195
9	CVE-2024-44083	- Điểm CVSS: 7.5 (Trung bình) - Ảnh hưởng: Hex-Rays IDA Pro - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép - Lỗ hổng chưa có mã khai thác và chưa bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-44083
10	CVE-2024-6670	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: WhatsUp Gold - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-6670

Thống 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 **40.171** (giảm so với tuần trước **41.844**) 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.

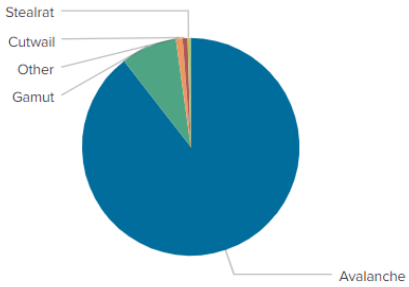


Tấn công Web

Trong tuần, có **81** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 72 trường hợp tấn công lừa đảo (Phishing), 09 trường hợp tấn công cài cắm mã độc.

Botnet

Trên thế giới có nhiều địa chỉ IP/domain độc hại được các nhóm đối tượng tấn công sử dụng làm máy chủ C&C trong botnet. Những địa chỉ này cho phép nhóm đối tượng điều khiển thiết bị thuộc các mạng botnet để thực hiện các hành vi trái phép như triển khai tấn công DDoS, phát tán mã độc, gửi thư rác, truy cập và đánh cắp dữ liệu trên thiết bị. Trong tuần, ghi nhận **20** địa chỉ IP/domain thuộc botnet có ảnh hưởng tới người dùng Việt Nam.



Địa chỉ được sử dụng trong các mạng botnet

differentia.ru	restless.su
disorderstatus.ru	andall.servicesql.info
atomictrivia.ru	www.marketingsay.com
amnsreiuojy.ru	vcbbcdipdxmu.me.uk
hzmksreiuojy.ru	tsfldbn.com
xjpakmdcfuqe.biz	sirec.in
restlesz.su	rikip.com
xjpakmdcfuqe.com	mvxycevi.info
xjpakmdcfuqe.in	jkaxlrkxqwsixubfu.org
xjpakmdcfuqe.ru	griefcube.cc

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **774** 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 các tổ chức, doanh nghiệp, nhà cung cấp, dịch vụ lớn như: Các mạng xã hội, ngân hàng, thư điện tử,...

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

STT	Website lừa đảo	Ghi chú
1	https://nhanvienghtk[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
2	https://vn[.]congtygiaohangtietkiemvn[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
3	https://giaohangtietkiem247[.]top	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
4	https://dichvu[.]congtygiaohangtietkiemvn[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
5	https://giaohangtietkiemvn[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
6	https://hethongnoibo[.]bio[.]link	Website giả mạo sàn TMĐT Lazada
7	https://hethongnoibo[.]bio[.]link	Website giả mạo sàn TMĐT Lazada
8	https://lazada68[.]com	Website giả mạo sàn TMĐT Lazada
9	https://www[.]baovietvc[.]top	Website giả mạo Ngân hàng TMCP Bảo Việt
10	https://sendovn[.]shop	Website giả mạo sàn TMĐT Sendo
11	https://kpd63519s[.]com	Website giả mạo sàn TMĐT Shopee
12	https://558-558-559[.]com	Website giả mạo sàn TMĐT Shopee
13	nzx65821s[.]com	Website giả mạo sàn TMĐT Shopee
14	https://tikimuasam24h[.]com	Website giả mạo sàn TMĐT Tiki
15	https://sjfku11[.]com	Website giả mạo sàn TMĐT Tiki
16	https://hethongtikicareers24h[.]com	Website giả mạo sàn TMĐT Tiki
17	https://hethongtikicareers24[.]com	Website giả mạo sàn TMĐT Tiki
18	https://sjfku88[.]com	Website giả mạo sàn TMĐT Tiki
19	https://chinhphu[.]dulieucutru[.]org	Website giả mạo Văn phòng Chính phủ
20	https://vnpttechnology[.]weebly[.]com	Website giả mạo VNPT- Tập đoàn Bưu chính Viễn thông Việt Nam

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, các đơn vị chủ động cập nhật các thông tin về các rủi ro an toàn thông tin mạng tại địa chỉ https://alert.khonggianmang.vn..

***

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**, Đề nghị các đơn vị, tổ chức, doanh nghiệp cần chủ động rà quét, phát hiện sớm các website lừa đảo giả mạo tổ chức của mình, cảnh báo sớm đến người dùng của nhằm ngăn chặn các hoạt động lừa đảo đến người dùng, đảm bảo an toàn thông tin cho người dùng, bảo vệ chính thương hiệu của tổ chức.

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