NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 36 (02/09/2024 – 08/09/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Cảnh báo:** Cisco phát hành bản vá cho lỗ hổng leo thang đặc quyền root đã có mã khai thác.

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: 462** 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

"Cảnh báo: Cisco phát hành bản vá cho lỗ hổng leo thang đặc quyền root đã có mã khai thác"

Cisco vừa phát hành bản vá cho một lỗ hổng command injection đã có mã khai thác công khai, cho phép đối tượng tấn công leo thang đặc quyền lên quyền root trên các hệ thống bị ảnh hưởng.

Lỗ hổng này có mã định danh CVE-2024-20469, tồn tại trên giải pháp Identity Services Engine (ISE) của Cisco – một phần mềm kiểm soát truy cập mạng dựa trên danh tính và thi hành chính sách, giúp quản lý thiết bị mạng và truy cập điểm cuối trong môi trường doanh nghiệp.

Nguyên nhân của lỗ hổng là do quá trình xác thực dữ liệu đầu vào của người dùng không đủ chặt chẽ. Đối tượng tấn công cục bộ có thể khai thác lỗ hổng này bằng cách gửi các lệnh CLI độc hại trong một cuộc tấn công có độ phức tạp thấp mà không cần sự tương tác của người dùng. Tuy nhiên, Cisco cho biết, lỗ hổng này chỉ có thể bị khai thác thành công nếu đối tượng tấn công đã có quyền Quản trị viên trên hệ thống chưa được vá.

Cisco cho biết hiện mã khai thác đã có sẵn, nhưng chưa có bằng chứng nào cho thấy lỗ hổng này bị khai thác ngoài thực tế. Hãng cũng cảnh báo rằng một tài khoản backdoor trong phần mềm Smart Licensing Utility Windows đã bị loại bỏ, vì tài khoản này có thể bị lợi dụng để đăng nhập vào các hệ thống chưa vá với quyền quản trị viên.

Trong năm 2024, Cisco cũng đã phát hành các bản vá cho các lỗ hổng nghiêm trọng khác, bao gồm lỗ hổng CVE-2024-20295 trên Integrated Management Controller (IMC), cho phép đối tượng tấn công leo thang đặc quyền lên quyền root; và lỗ hổng CVE-2024-20401, cho phép đối tượng tấn công thêm tài khoản root giả mạo và gây crash vĩnh viễn hệ thống Security Email Gateway (SEG) thông qua email độc hại. Một lỗ hổng khác trên Cisco Smart Software Manager On-Prem (Cisco SSM On-Prem) cũng đã được cảnh báo, cho phép đối tượng tấn công thay đổi mật khẩu của bất kỳ người dùng nào trên hệ thống.

Nguồn: https://www.bleepingcomputer.com/news/security/cisco-fixes-root-escalation-vulnerability-with-public-exploit-code/?&web_view=true

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 **505** lỗ hổng, trong đó có 196 lỗ hổng mức Cao, 231 lỗ hổng mức Trung bình, 10 lỗ hổng mức Thấp và 68 lỗ hổng chưa đánh giá. Trong đó có ít nhất 78 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 Zyxel, Kingsoft và Google, cụ thể là như sau:

- **CVE-2024-7261 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên thiết bị mạng của hãng Zyxel cho phép đối tượng tấn công thực thi mã từ xa do lỗi tại quá trình lọc tham số "host" của chương trình CGI không đảm bảo bảo mật. Hiện lỗ hổng chưa có mã khai thác và chưa được khai thác bởi các nhóm tấn công trong thực tế.
- **CVE-2024-7262 (Điểm CVSS: 7.8 – Cao):** Lỗ hổng tồn tại trên Kingsoft WPS Office cho phép đối tượng tấn công nạp một thư viện Windows tùy ý, dẫn tới việc hệ thống bị thỏa hiệp, qua đó cho phép đối tượng tấn công thực thi mã từ xa, leo thang đặc quyền, truy cập và thực hiện các hành vi trái phép. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác bởi các nhóm tấn công trong thực tế như APT-C-60.
- **CVE-2024-7971 (Điểm CVSS: 8.8 – Cao):** Lỗ hổng tồn tại trên Google Chrome cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép trên hệ thống sau khi khai thác lỗi heap corruption sử dụng một trang HTML độc hại. Hiện lỗ hổng đã có mã khai tác và đang bị khai thác trong thực tế bởi các nhóm tấn công như Lazarus Group.

TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	CVE-2024-7261	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Zyxel - 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-2024-7261
2	CVE-2024-7262	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Kingsoft WPS Office - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa, leo thang đặc quyền, truy cập và thực hiện 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-2024-7262
3	CVE-2024-7971	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Google Chrome - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện 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-2024-7971
4	CVE-2024-1212	- Điểm CVSS: 10.0 (Nghiêm trọng) - Ảnh hưởng: LoadMaster - 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-2024-1212
5	CVE-2024-30051	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Microsoft Windows 10, Windows 11 - Mô tả: Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền - 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-2024-30051

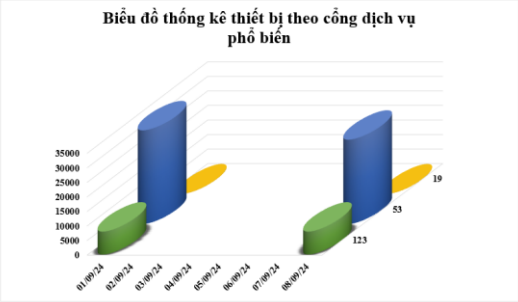
TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-34102	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Adobe Commerce - 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 trusssòng thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-34102
7	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
8	CVE-2024-38063	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Microsoft Windows 10, Windows Server 2022 - 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-2024-38063
9	CVE-2024-25641	- Điểm CVSS: 9.1 (Nghiêm trọng) - Ảnh hưởng: Cacti - 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-2024-25641
10	CVE-2024-28987	- Điểm CVSS: 9.1 (Nghiêm trọng) - Ảnh hưởng: SolarWinds Web Help Desk - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện 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-2024-28987

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 **36.907** (giảm so với tuần trước **40.171**) 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.

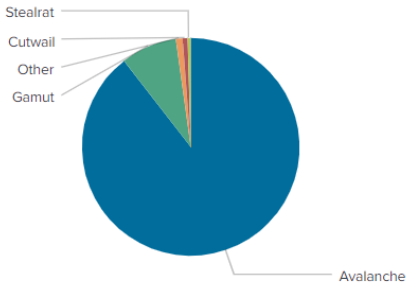


Tấn công Web

Trong tuần, có **80** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 73 trường hợp tấn công lừa đảo (Phishing), 07 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	spaines.pw
amnsreiuojy.ru	wdxzlv.org
hzmksreiuojy.ru	griefcube.cc
xjpakmdcfuqe.biz	db2017417b23.zapto.org
restlesz.su	zoneshewa.net
xjpakmdcfuqe.in	yxjsibeugmmj.com
xjpakmdcfuqe.ru	yobuqokipnfaxkeor.net
xjpakmdcfuqe.com	xprzkwzu.net

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **462** 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://giaohangtietkiem247[.]top	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
2	https://dichvu[.]congtygiaohangtietkiemvn[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
3	https://giaohangtietkiemvn[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
4	https://org[.]govqp[.]com	Website giả mạo Cục Đăng kiểm Việt Nam
5	https://play[.]appgoogle[.]cc	Website giả mạo Google
6	https://hethongnoibo[.]bio[.]link	Website giả mạo sàn TMĐT Lazada
7	https://lazada68[.]com	Website giả mạo sàn TMĐT Lazada
8	https://baovietcv[.]top	Website giả mạo Ngân hàng TMCP Bảo Việt
9	https://www[.]baovietvc[.]top	Website giả mạo Ngân hàng TMCP Bảo Việt
10	https://tienichshiinhan[.]com	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
11	https://sendovn[.]shop	Website giả mạo sàn TMĐT Sendo
12	https://kpd63519s[.]com	Website giả mạo sàn TMĐT Shopee
13	https://558-558-559[.]com	Website giả mạo sàn TMĐT Shopee
14	nzx65821s[.]com	Website giả mạo sàn TMĐT Shopee
15	https://muasamtiki24h[.]com	Website giả mạo sàn TMĐT Tiki
16	https://sjfku11[.]com	Website giả mạo sàn TMĐT Tiki
17	https://hethongtikicareers24h[.]com	Website giả mạo sàn TMĐT Tiki
18	https://hethongtikicareers24[.]com	Website giả mạo sàn TMĐT Tiki
19	https://sjfku88[.]com	Website giả mạo sàn TMĐT Tiki
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