BỘ CÔNG AN
CÔNG AN TỈNH QUẢNG NGÃI

Số: 3002 /CAT-ANM

V/v cảnh báo lỗ hổng bảo mật nghiêm trọng tháng 9/2025

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Quảng Ngãi, ngày 20 tháng 10 năm 2025

Kính gửi:
- Ủy ban Mặt trận Tổ quốc Việt Nam tỉnh;
- Văn phòng Tỉnh ủy, UBND tỉnh;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Các sở, ban ngành và hội đoàn thể tỉnh;
- Bộ Chỉ huy Quân sự tỉnh; Tòa án nhân dân tỉnh;
- Viện Kiểm sát nhân dân tỉnh; Thi hành án dân sự tỉnh;
- Bảo hiểm xã hội tỉnh; Cảng vụ Hàng hải Quảng Ngãi;
- Thống kê tỉnh; Thuế tỉnh Quảng Ngãi;
- Kho bạc Nhà nước khu vực XV;
- Báo và Phát thanh, Truyền hình Quảng Ngãi;
- Các Trường: Đại học Phạm Văn Đồng, Cao đẳng Kon Tum, Cao đẳng Việt Nam - Hàn Quốc - Quảng Ngãi;
- Công ty CP Lọc hóa dầu Bình Sơn; Truyền tải điện Quảng Ngãi; Điện lực Quảng Ngãi;
- UBND các xã, phường, Đặc khu Lý Sơn.

Trong tháng 9/2025, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an đã thực hiện phân tích và tổng hợp đối với **11** lỗ hổng bảo mật nghiêm trọng ảnh hưởng đến hệ thống thông tin của Việt Nam *(Tài liệu lưu hành nội bộ)*. Trong đó, có 03 lỗ hổng bảo mật có mức độ rất nghiêm trọng; 06 lỗ hổng bảo mật nghiêm trọng; 02 lỗ hổng bảo mật mức trung bình, cụ thể:

1. Lỗ hổng bảo mật trên hệ điều hành của Microsoft

1.1. CVE-2025-55232 - Lỗ hổng thực thi mã từ xa của Microsoft High Performance Compute (HPC) Pack

- Mô tả:

+ Điểm CVSS: 9.8/10;

+ Mức độ: Rất nghiêm trọng;

+ Lỗ hổng bảo mật đã được phát hiện trong Microsoft High Performance Compute Pack (HPC) liên quan đến việc hủy tuần tự hóa dữ liệu không đáng tin cậy. Lỗ hổng này cho phép tin tặc thực thi mã tùy ý qua mạng, có khả năng dẫn đến xâm phạm toàn bộ hệ thống.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến gói Microsoft HPC 2019 phiên bản từ 1.0.0 đến 6.4.8352.

- Khuyến nghị: Microsoft đã xử lý lỗ hổng này trong bản cập nhật Patch Tuesday tháng 9 năm 2025. Bản sửa lỗi này nằm trong số 80 lỗ hổng bảo mật khác

đã được vá trong cùng bản phát hành. Các tổ chức được khuyến cáo nên áp dụng bản cập nhật bảo mật ngay lập tức. Thông tin chi tiết: https://msrc.microsoft.com/update-quide/vulnerability/CVE-2025-55232.

- Lỗ hổng chưa có PoC công khai.

1.2. CVE-2025-54914 - Lỗ hổng nâng cao đặc quyền của Microsoft Azure Networking

- Mô tả:

+ Điểm CVSS: 10/10;

+ Mức độ: Rất nghiêm trọng;

+ Lỗ hổng do API "GetRouteTable" của dịch vụ Mạng Azure cho phép máy khách có quyền đọc trên mạng ảo tạo các "routing" mới bên trong cùng một mạng con mà không cần xác minh xem người gọi có được ủy quyền cho hành động đó hay không. Dẫn đến việc leo thang đặc quyền cho phép tin tặc kiểm soát hoàn toàn các tài nguyên mạng Azure mà không cần bất kỳ tương tác nào của người dùng.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến tất cả phiên bản Windows có dịch vụ mạng Microsoft Azure.

- Khuyến nghị: Microsoft khuyến cáo người dùng nên áp dụng bản vá do Microsoft phát hành vào ngày 05/9/2025 để bổ sung tính năng kiểm tra đặc quyền rõ ràng bên trong đường dẫn API "GetRouteTable". Hoặc có thể cấu hình Azure Monitor để cảnh báo về bất kỳ routing mới nào được tạo bằng GUID không xác định - cho biết khả năng có nỗ lực leo thang đặc quyền. Thông tin chi tiết: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-54914.

- Lỗ hổng có PoC: https://github.com/mrk336/Azure-Networking-Privilege-Escalation-Exploit-CVE-2025-54914.

2. Lỗ hổng bảo mật phần mềm trên hệ điều hành Linux

*** CVE-2025-38501** - Lỗ hổng trong hệ thống KSMBD của Kernel Linux

- Mô tả:

+ Điểm CVSS: 6.8/10;

+ Mức độ: Trung bình;

+ Lỗ hổng này phát sinh từ cách hệ thống KSMBD xử lý các kết nối TCP. Bằng cách khởi tạo một giao thức bắt tay TCP ba bước nhưng cố tình không hoàn tất phiên, tin tặc có thể buộc máy chủ KSMBD phải giữ các kết nối nửa mở này vô thời hạn, dẫn tới tình trạng cạn kiệt tài nguyên máy chủ và gây ra tình trạng từ chối dịch vụ (DoS).

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến kernel linux từ phiên bản 5.3.

- Khuyến nghị: Nhà phát hành đã phát hành bản vá lỗi trong Linux Kernel 6.1.15 trở lên. Quản trị viên được khuyến khích cập nhật ngay lập tức. Đối với

những môi trường không thể vá lỗi ngay lập tức, khuyến nghị thực hiện các biện pháp giảm thiểu sau:

+ Nâng cấp lên Linux Kernel 6.1.15+: Áp dụng bản vá ngược dòng (cam kết e6bb9193974059ddbb0ce7763fa3882bd60d4dc3) để thực thi giới hạn tồn đọng và thử lại TCP nghiêm ngặt hơn.

+ Hạn chế tiếp xúc với cổng 445: Sử dụng tường lửa để hạn chế việc tiếp xúc dịch vụ SMB với các mạng nội bộ đáng tin cậy.

+ Gói SYN giới hạn tốc độ: Triển khai giới hạn tốc độ ở lớp mạng để giảm thiểu các nỗ lực tấn công tràn SYN vào cổng 445.

+ Giám sát hành vi mạng bất thường: Phát hiện các đột biến bất thường trong lưu lượng gói tin SYN, có thể chỉ ra các nỗ lực khai thác.

+ Điều chỉnh cài đặt KSMBD: Giảm handshake_timeout và cấu hình số lượng trong không gian người dùng để giảm bề mặt tấn công.

- Lỗ hổng có PoC: https://github.com/keymaker-arch/KSMBDrain.

3. Lỗ hổng bảo mật phần mềm trên tường lửa

*** CVE-2025-37125** - Lỗ hổng Firewall trong hệ điều hành HPE Aruba Networking EdgeConnect

- Mô tả:

+ Điểm CVSS: 7.5/10;

+ Mức độ: Nghiêm trọng;

+ Việc khai thác thành công có thể cho phép tin tặc vượt qua các biện pháp bảo vệ tường lửa, có khả năng dẫn đến việc xử lý lưu lượng truy cập trái phép không đúng cách, xâm phạm tính bảo mật của sản phẩm bằng cách giành được đặc quyền, đọc thông tin nhạy cảm, thực thi lệnh, trốn tránh phát hiện, v.v.

- Phiên bản ảnh hưởng: Lỗ hổng này ảnh hưởng đến cổng SD-WAN HPE Aruba Networking EdgeConnect phiên bản 9.5.XX: 9.5.3.X trở xuống.

- Khuyến nghị: Nhà phát hành HPE Aruba Networking đã phát hành bản vá cho HPE Aruba Networking EdgeConnect SD-WAN Gateways để giải quyết lỗ hổng bảo mật này. Thông tin chi tiết về bản cập nhật có trong: https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04943en us&d ocLocale=en US.

- Lỗ hổng chưa có PoC công khai.

4. Lỗ hổng bảo mật phần mềm trên dịch vụ Web

4.1. CVE-2025-8671 - Lỗ hổng trên HTTP/2 cho phép tấn công DoS

- Mô tả:

+ Điểm CVSS: 7.5/10;

+ Mức độ: Nghiêm trọng;

+ Lỗ hổng xảy ra do số lượng máy chủ đặt ra số yêu cầu HTTP/2 đồng thời trên mỗi kết nối TCP từ máy khách không khớp với kiến trúc nội bộ của một số triển khai HTTP/2. Tin tặc có thể gửi hàng nghìn yêu cầu, tạo ra tình trạng từ chối dịch vụ đối với người dùng hợp pháp, có thể dẫn đến sự cố hết bộ nhớ.

- Phiên bản ảnh hưởng: Lỗ hổng bảo mật này ảnh hưởng đến nhiều máy chủ và thư viện như: Apache Tomcat, Netty, Varnish, Fastly, F5, SUSE, Wind River.

- Khuyến nghị: Nhà phát hành khuyến cáo người dùng áp dụng ngay các bản cập nhật bảo mật do nhà cung cấp phát hành, bao gồm: Apache Tomcat, Netty, Varnish, F5, Fastly và SUSE. Việc tạm thời vô hiệu hóa HTTP/2 hoặc định tuyến lưu lượng qua HTTP/1.1 có thể giảm thiểu rủi ro. Áp dụng xác thực giao thức nghiêm ngặt hơn - loại bỏ hoặc xử lý các khung WINDOW-UPDATE, PRIORITY hoặc khung điều khiển bị lỗi là lỗi kết nối thay vì lỗi luồng. Triển khai giới hạn tốc độ khung điều khiển, tốc độ/giới hạn kết nối cho mỗi máy khách và giám sát các bất thường như tạo RST-STREAM cao hoặc các mẫu xử lý yêu cầu không khớp. Phát hiện tự động kết hợp với việc định hình lưu lượng hoặc chặn các kết nối vi phạm có thể giảm thiểu rủi ro cho đến khi bản vá được vá hoàn toàn.

- Lỗ hổng có PoC: https://github.com/nomi-sec/PoC-in-GitHub/blob/master/2025/CVE-2025-8671.json.

4.2. CVE-2025-57833 - Lỗ hổng SQL Injection ảnh hưởng các ứng dụng web Django

- Mô tả:

+ Điểm CVSS: 7.1/10;

+ Mức độ: Nghiêm trọng;

+ Lỗ hổng này xảy ra khi dữ liệu đầu vào chưa được kiểm tra của người dùng được sử dụng làm khóa từ điển trong annotated() hoặc alias() với FilteredRelation. Có thể dẫn đến truy cập dữ liệu trái phép, giả mạo hoặc thậm chí xâm phạm toàn bộ cơ sở dữ liệu ứng dụng.

- Phiên bản ảnh hưởng: Lỗ hổng bảo mật này ảnh hưởng đến các phiên bản Django 4.2, 5.1 và 5.2.

- Khuyến nghị: Django Software Foundation đã phát hành các bản cập nhật bảo mật quan trọng cho nhiều phiên bản được hỗ trợ của nền tảng web Python phổ biến. Thông tin chi tiết bản cập nhật: https://www.djangoproject.com/weblog/2025/sep/03/security-releases/

- Lỗ hổng có PoC: https://qithub.com/Mkway/CVE-2025-57833

5. Lỗ hổng bảo mật phần mềm trên dịch vụ Email

* **CVE-2025-53859** - Lỗ hổng ghi đè bộ nhớ trên NGX Mail SMTP trong NGINX

- Mô tả:

+ Điểm CVSS: 6.3/10;

+ Mức độ: Trung bình;

+ Lỗ hổng này cho phép tin tặc thực hiện việc đọc đè bộ nhớ quy trình xác thực SMTP của NGINX, có khả năng dẫn đến rò rỉ thông tin nhạy cảm thông qua yêu cầu HTTP đến máy chủ xác thực. Phía máy chủ có thể rò rỉ các byte tùy ý được gửi trong yêu cầu đến máy chủ xác thực.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến NGINX phiên bản từ 0.7.22 đến 1.29.0.

- Khuyến nghị: Lỗ hổng bảo mật đã được khắc phục trong NGINX phiên bản 1.29.1. Đối với các phiên bản cũ hơn, có hai giải pháp tạm thời: vô hiệu hóa tham số 'none' trong chỉ thị 'smtp_auth' hoặc xóa dòng tiêu đề 'Auth-Wait' trong phản hồi của máy chủ xác thực. Bản vá cho sự cố này có sẵn tại https://nqinx.org/download/patch.2025.smtp.txt.

- Lỗ hổng chưa có PoC công khai.

6. Lỗ hổng bảo mật phần mềm trên ngôn ngữ lập trình

*** CVE-2025-59340** - Lỗ hổng bỏ qua Sandbox trong Jinjava Engine của HubSpot

- Mô tả:

+ Điểm CVSS: 9.8/10;

+ Mức độ: Rất nghiêm trọng;

+ Lỗ hổng nghiêm trọng trong Sandbox Jinjava cho phép tin tặc thoát khỏi sandbox và khởi tạo nhiều lớp bằng JavaType. Và cho phép tin tặc đọc các tệp tùy ý (chẳng hạn như /proc/self/environ) và thực hiện giả mạo yêu cầu phía máy chủ (SSRF) bằng cách tạo các đối tượng liên quan đến mạng.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến các phiên bản jinjava từ 2.8.1 trở xuống.

- Khuyến nghị: Nhà phát triển đưa ra biện pháp giảm thiểu như: cập nhật lên phiên bản mới nhất của Jinjava; áp dụng các bản vá bảo mật từ khuyến cáo chính thức; xem xét và hạn chế khả năng khởi tạo lớp Java; triển khai các hạn chế sandbox bổ sung; tiến hành kiểm tra bảo mật kỹ lưỡng các triển khai Jinjava; giám sát các nỗ lực khai thác tiềm ẩn. Thông tin bản cập nhật: https://github.eom/HubSpot/jinjava/releases/tag/jinjava-2.8.1.

- Lỗ hổng có PoC: https://github.com/HubSpot/jinjava.

7. Lỗ hổng bảo mật phần mềm trên trình duyệt

*** CVE-2025-10585** - Lỗ hổng Zero Day trong công cụ JavaScript và WebAssembly V8 trên Chrome.

- Mô tả:

+ Điểm CVSS: 8.8/10;

+ Mức độ: Nghiêm trọng;

+ Lỗ hổng này là lỗi nhầm lẫn kiểu trong công cụ JavaScript và WebAssembly V8 có thể cho phép tin tặc đánh lừa trình duyệt về các loại đối tượng, có khả năng dẫn đến việc thực thi mã tùy ý, trình duyệt bị sập hoặc xâm phạm toàn bộ hệ thống trong trường hợp nghiêm trọng.

- Phiên bản ảnh hưởng: Lỗ hổng bảo mật này ảnh hưởng đến các phiên bản Google Chrome trước 140.0.7339.185.

- Khuyến nghị: Nhà phát hành khuyến nghị người dùng nên cập nhật trình duyệt Chrome lên phiên bản 140.0.7339.185/.186 cho Windows và Apple macOS, và 140.0.7339.185 cho Linux. Để đảm bảo các bản cập nhật mới nhất đã được cài đặt, người dùng có thể truy cập mục Thêm > Trợ giúp > Giới thiệu về Google Chrome và chọn Khởi chạy lại. Để biết thêm thông tin chi tiết, vui lòng tham khảo: https://chromereleases.googleblog.com/2025/Q9/stable-channel-update-for-desktop17.html.

- Lỗ hổng chưa có PoC công khai.

8. Lỗ hổng bảo mật chuỗi cung ứng khác

8.1. CVE-2025-43300 - Lỗ hổng trong bộ nhớ xử lý hình ảnh DNG của iOS/macOS

- Mô tả:

+ Điểm CVSS: 8.8/10;

+ Mức độ: Nghiêm trọng;

+ Lỗ hổng này tồn tại trong mã giải nén JPEG Lossless trong RawCamera.bundle, được kích hoạt bởi sự không nhất quán giữa siêu dữ liệu TIFF và các tham số luồng JPEG trong tệp DNG. Việc khai thác thành công lỗ hổng này có thể cho phép tin tặc thực thi mã tùy ý bằng các tệp hình ảnh.

- Phiên bản ảnh hưởng: Lỗ hổng bảo mật này ảnh hưởng đến các phiên bản iOS trước 18.6.2, phiên bản iPadOS trước 18.6.2, phiên bản iPadOS trước 17.7.10, phiên bản macOS Sonoma trước 14.7.8, phiên bản macOS Ventura trước 13.7.8, phiên bản macOS Sequoia trước 15.6.1.

- Khuyến nghị: Apple thông báo lỗ hổng đã được khắc phục trong iOS 15.8.5 và iPadOS 15.8.5, iOS 16.7.12 và iPadOS 16.7.12. Người dùng và quản trị viên của các phiên bản sản phẩm bị ảnh hưởng được khuyến cáo nên cập nhật lên phiên bản mới nhất ngay lập tức. Thông tin bản cập nhật có trong: https://support.apple.com/en-us/124925.

- Lỗ hổng có PoC: https://github.com/hunters-sec/CVE-2025-43300.

8.2. CVE-2025-21043 - Lỗ hổng thực thi mã từ xa trên các thiết bị Android của Samsung

- Mô tả:

+ Điểm CVSS: 8.8/10;

+ Mức độ: Nghiêm trọng;

+ Lỗ hổng này xảy ra do lỗi ghi ngoài giới hạn trong libimagecodec.quram.so. Việc khai thác thành công lỗ hổng này có thể cho phép tin tặc chưa xác thực thực thi mã độc từ xa trên thiết bị bị tấn công.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng tới các phiên bản Android 13, 14,15 và 16.

- Khuyến nghị: Samsung đã phát hành bản cập nhật bảo mật để giải quyết lỗ hổng zero-day nghiêm trọng trên các thiết bị Samsung. Người dùng các phiên bản sản phẩm bị ảnh hưởng được khuyến cáo nên cập nhật lên phiên bản mới nhất ngay lập tức. Thông tin bản cập nhật: https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=09.

- Lỗ hổng chưa có PoC công khai.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin góp phần bảo đảm an toàn các cơ quan, đơn vị trên địa bàn tỉnh, Công an tỉnh đề nghị lãnh đạo các đơn vị tiếp tục chỉ đạo rà soát, cập nhật, vá lỗi hệ thống, tăng cường triển khai các biện pháp giám sát liên tục các hệ thống thông tin, phát hiện sớm các dấu hiệu bất thường, tấn công mạng. Trong quá trình thực hiện nếu có khó khăn, vướng mắc kịp thời liên hệ Công an tỉnh *(qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, số điện thoại 088.830.9485)* để được hướng dẫn.

Đề nghị các đồng chí quan tâm chỉ đạo thực hiện./.

Nơi nhận:
- Như trên;
- UBND tỉnh (báo cáo);
- Giám đốc Công an tỉnh;
- Phòng Tham mưu;
- Lưu: VT, ANM.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Đại tá Võ Văn Dương