BỘ CÔNG AN
CÔNG AN TỈNH QUẢNG NGÃI

Số: 1766 /CAT-ANM

V/v cảnh báo lỗ hổng bảo mật nghiêm trọng tháng 8/2025

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

Quảng Ngãi, ngày 09 tháng 9 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;
- Bộ Chỉ huy Quân sự tỉnh; Cục Thi hành án dân sự tỉnh;
- Viện Kiểm sát nhân dân tỉnh; Tòa án nhân dân tỉnh;
- Chi Cục Thống kê tỉnh; Bảo hiểm xã hội tỉnh; Thuế tỉnh;
- Kho bạc Nhà nước tỉnh; Cảng vụ Hàng hải tỉnh;
- Các sở, ban ngành và hội đoàn thể tỉnh;
- UBND các xã, phường, đặc khu;
- 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.

Trong tháng 8/2025, 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 **10** 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 05 lỗ hổng bảo mật có mức độ rất nghiêm trọng; 04 lỗ hổng bảo mật nghiêm trọng; 01 lỗ hổng bảo mật mức trung bình (trong đó 05 lỗ hổng có PoC công khai), cụ thể:

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

*** CVE-2025-50165** – Lỗ hổng thực thi mã từ xa do Windows Graphics Componet.

- Mô tả:

+ Điểm CVSS: 9.8/10;

+ Mức độ: Critical;

+ Lỗ hổng thực thi mã từ xa cho phép tin tặc thực thi mã từ xa trên hệ thống mục tiêu thông qua một hình ảnh JPEG được tạo đặc biệt (có thể được nhúng trong Office hoặc các tệp khác) do tham chiếu con trỏ không đáng tin cậy trong thành phần Microsoft Graphics.

- Phiên bản ảnh hưởng: Các phiên bản Windows 11 Version 24h2, Windows Server 2025 trước 10.0.26100.4946.

- Khuyến nghị: Microsoft đã báo cáo rằng lỗ hổng này đã được giảm thiểu hoàn toàn và người dùng nên cập nhật lên phiên bản hệ điều hành mới nhất. Hướng

dẫn cập nhật: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025- 50165.

- Lỗ hổng có PoC: https://github.com/allinsthon/CVE-2025-50165

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

* **CVE-2025-46809** - Lổ hổng chèn thông tin vào tệp nhật ký trong SUSE Multi Linux Manager.

- Mô tả:

+ Điểm CVSS: 6.9/10;

+ Mức độ: Medium;

+ Tin tặc có thể khai thác lỗ hổng này bằng cách chèn một số thông tin đặc biệt vào tệp nhật ký trong SUSE Multi Linux Manager để lấy được tên người dùng và mật khẩu Proxy HTTP dạng văn bản rõ trong Repolog.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến Container suse/manager/5.0/x86_64/server:5.0.5.7.30.1 các phiên bản trước 5.0.27-150600.3.33.1.

- Khuyến nghị: Nhà phát hành đã khuyến cáo người dùng cập nhật hệ thống và các gói liên quan lên phiên bản vá mới nhất do SUSE phát hành, thông tin: https://www.tenable.com/plugins/nessus/242658.

- Lỗ hổng chưa có PoC công khai.

3. Lỗ hổng bảo mật phần mềm trên tường lửa

* **CVE-2025-20265** - Lỗ hổng trong Phần mềm Trung tâm quản lý tường lửa an toàn Cisco (FMC).

- Mô tả:

+ Điểm CVSS: 10/10;

+ Mức độ: Critical;

+ Lỗ hổng này là do việc xử lý dữ liệu đầu vào của người dùng không đúng cách trong giai đoạn xác thực. Tin tặc có thể khai thác lỗ hổng này bằng cách gửi dữ liệu đầu vào giả mạo khi nhập thông tin đăng nhập sẽ được xác thực tại máy chủ RADIUS đã cấu hình. Khi lỗ hổng khai thác thành công có thể cho phép tin tặc thực thi các lệnh ở mức đặc quyền cao.

- Phiên bản ảnh hưởng: Lỗ hổng này ảnh hưởng đến các phiên bản Cisco Secure FMC Software 7.0.7 và 7.7.0 nếu bật xác thực RADIUS.

- Khuyến nghị: Người dùng và quản trị viên nên cập nhật phiên bản mới nhất ngay lập tức. Nếu việc vá lỗi không khả thi, người dùng nên chuyển sang hình thức xác thực thay thế, chẳng hạn như tài khoản người dùng cục bộ, xác thực giao thức truy cập thư mục nhẹ (LDAP) bên ngoài hoặc đăng nhập một lần ngôn ngữ đánh dấu xác nhận bảo mật (SAML SSO). Để biết thêm thông tin chi tiết từ nhà phát hành: https://sec.cloudapps.cisco.com/securitv/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-radius-rce-TNBKf79.

- Lỗ hổng có PoC: https://github.com/jordan922/cve2025-20265.

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

*** CVE-2025-53767** – Lỗ hổng nâng cao đặc quyền trên Microsoft Azure OpenAI.

- Mô tả:

+ Điểm CVSS: 10/10;

+ Mức độ: Critical;

+ Lỗ hổng giả mạo yêu cầu phía máy chủ (SSRF) trong các dịch vụ Azure OpenAI xảy ra khi tin tặc có thể thao túng máy chủ đưa ra các yêu cầu tùy ý đến các tài nguyên bên trong hoặc bên ngoài, thường bỏ qua phân đoạn mạng và kiểm soát bảo mật. Trong trường hợp này, lỗ hổng cho phép nâng cao đặc quyền, cho phép tin tặc vượt qua các cơ chế xác thực và ủy quyền trong môi trường Azure OpenAI.

- Phiên bản ảnh hưởng**:** Các phiên bản ảnh hưởng không được nhà phát hành công bố.

- Khuyến nghị: Microsoft đã phát hành bản vá bảo mật để trong bản cập nhật đế giải quyết lỗ hổng. Người dùng không cần phải thực hiện bất kỳ hành động nào. Thông tin về bản cập nhật: https://msrc.microsoft.com/update guide/vulnerabilitv/CVE-2025-53767.

- Lỗ hổng chưa có PoC công khai.

*** CVE-2025-5394** – Lỗ hổng trong WordPress Theme gây mất quyền điều khiển Web.

* Mô tả:

+ Điểm CVSS: 9.8/10;

+ Mức độ: Critical;

+ Tin tặc có thể tải lên các tệp zip chứa webshell được ngụy trang thành plugin để thực thi mã từ xa do việc thiếu kiểm tra khả năng của hàm alone_import_pack_install_plugin() trong giao diện Alone - Charity Multipurpose Non-profit WordPress Theme dành cho WordPress.

- Phiên bản ảnh hưởng: Lỗ hổng bảo mật này ảnh hưởng đến WordPress Theme, Alone, phiên bản 7.8.3 trở về trước.

- Khuyến nghị: Quản trị viên trang web đang sử dụng giao diện Alone nên cập nhật ngay lên phiên bản 7.8.4 trở lên, phiên bản này có chứa bản vá bảo mật. Nhà phát hành đã khắc phục lỗ hổng này trong bản phát hành mới nhất có sẵn trên ThemeForest: https://themeforest.net/item/alone-charity-multipurpose-nonprofit-wordpress-theme/15019939

- Lỗ hổng có PoC: https://github.com/fokda-prodz/CVE-2025-5394.

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

* **CVE-2025-53786** – Lỗ hổng nâng cao đặc quyền trong Microsoft Exchange Server.

- Mô tả:

+ Điểm CVSS: 8/10;

+ Mức độ: High;

+ Lỗ hổng nâng cao đặc quyền (EoP) ảnh hưởng đến việc triển khai kết hợp Microsoft Exchange Server. Kẻ tấn công có quyền quản trị viên đối với Exchange Server có thể leo thang đặc quyền trong môi trường đám mây được kết nối. Lỗ hổng này tồn tại do Exchange Server và Exchange Online chia sẻ "cùng một nguyên tắc dịch vụ trong cấu hình kết hợp".

+ Phiên bản ảnh hưởng: Microsoft Exchange Server 2016 bị ảnh hưởng từ phiên bản 15.02.0 đến trước 15.02.1748.024 và Microsoft Exchange Server 2019 bị ảnh hưởng từ phiên bản 15.02.0.0 đến trước 15.02.2562.017.

- Khuyến nghị: Microsoft đã phát hành bản sửa lỗi cải thiện bảo mật cho các triển khai Exchange hybrid, giúp giảm thiểu sự cố này. Để được bảo vệ toàn diện, người dùng nên áp dụng bản sửa lỗi hoặc phiên bản mới hơn. Ngoài ra, Microsoft khuyến nghị áp dụng các khuyến nghị cấu hình theo hướng dẫn https://learn.microsoft.com/vi-vn/Exchange/hybrid-deployment/deploy-dedicated-hybrid-app.

Ngoài ra, Microsoft khuyến nghị những khách hàng đã cấu hình xác thực Exchange hybrid hoặc OAuth cho Exchange Server thành Exchange Online và không còn sử dụng nữa nên đảm bảo rằng đã đặt lại "keyCredentials" của chủ thể dịch vụ. Để biết thêm thông tin từ Microsoft: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53786

- Lỗ hổng có PoC: https://github.com/barbaraeivyu/CVE-2025-53786.

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

* **CVE-2025-23319** – Lổ hổng bảo mật trong nềsn tảng Python trên NVIDIA Triton Inference Server.

- Mô tả:

+ Điểm CVSS: 8.1/10;

+ Mức độ: High;

+ Lỗ hổng bắt nguồn từ Python backend của máy chủ cho phép tin tặc vượt quá giới hạn bộ nhớ dùng chung bằng cách gửi một yêu cầu rất lớn. Việc khai thác thành công lỗ hổng này có thể dẫn đến việc tiết lộ thông tin. Từ đó có thể dẫn đến tấn công thực thi mã từ xa, chiếm quyền kiểm soát hoàn toàn máy chủ.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến các phiên bản NVIDIA Triton Inference Server và Python backend trước 25.07.

- Khuyến nghị: Nhà phát hành đưa ra biện pháp giảm thiểu chính là nâng cấp cả NVIDIA Triton Inference Server và Python backend lên phiên bản 25.07. Người

dùng có thể xem thông tin trong bản tin bảo mật của NVIDIA: https://nvidia.custhelp.com/app/answers/detail/a_id/5687.

- Lỗ hổng chưa có PoC công khai.

7. Lỗ hổng bảo mật phần mềm trên trình duyệt

*** CVE-2025-9132** – Lỗ hổng ghi ngoài giới hạn trong V8 của Google Chrome.

- Mô tả:

+ Điểm CVSS: 8.8/10;

+ Mức độ: High.

+ Tin tặc có thể khai thác lỗ hổng thông qua nội dung HTML được tạo ra trong các phiên duyệt web thông thường dẫn tới lỗi ghi ngoài giới hạn (bộ nhớ ngoài vùng đệm dự định có thể bị ghi đè). Khiến trình duyệt có thể làm hỏng bộ nhớ, thoát khỏi cơ chế bảo vệ sandbox, làm sập trình duyệt hoặc cho phép thực thi mã từ xa.

- Phiên bản ảnh hưởng: Lỗ hổng bảo mật này ảnh hưởng đến các phiên bản Google Chrome trước 138.0.7204.157.

- Khuyến nghị: Nhà phát hành thông báo bản sửa lỗi cho lỗ hổng V8 đã được đưa vào Chrome phiên bản 139.0.7258.138/.139 dành cho Windows và macOS, và phiên bản 139.0.7258.138 dành cho Linux, dự kiến sẽ sớm được cung cấp cho tất cả người dùng. Thông tin chi tiết: https://chromereleases.googleblog.com/2025/08/stable-channel-update-for-desktop_19.html.

- Lỗ hổng chưa có PoC công khai.

8. Lỗ hổng bảo mật chuỗi cung ứng khác

*** CVE-2025-8088** - Lỗ hổng Zero-Day thực thi mã từ xa trên WinRAR.

- Mô tả:

+ Điểm CVSS: 8.8/10;

+ Mức độ: High;

+ Lỗ hổng xảy ra khi giải nén một tệp phiên bản RAR dành cho Windows, UnRAR, mã nguồn UnRAR di động và UnRAR.dll có thể bị lừa sử dụng đường dẫn được xác định trong một kho lưu trữ được tạo đặc biệt, thay vì đường dẫn đã chỉ định. Tin tặc có thể khai thác để thực thi mã tùy ý bằng cách tạo các tệp lưu trữ độc hại.

- Phiên bản ảnh hưởng: Lỗ hổng bảo mật này ảnh hưởng đến các phiên bản WinRAR từ trước đến 7.12.

- Khuyến nghị: Nhà phát hành đã khắc phục lỗ hổng này trong WinRAR phiên bản 7.13 phát hành vào ngày 30 tháng 7 năm 2025. Người dùng cần cập nhật lên phiên bản mới nhất để tránh bị ảnh hưởng, thông tin về bản cập nhật và lỗ hổng: https://www.winrar.com/singlenewsview.html?&L=0&tx_ttnews%5Btt_news%5D=283&cHash=a64b4a8f662d3639dec8d65f47bc93c5.

- Lỗ hổng có PoC: https://github.com/jordan922/CVE-2025-8088

*** CVE-2025-49457** – Lỗ hổng leo thang đặc quyền trên ứng dụng Zoom.

- Mô tả:

+ Điểm CVSS: 9.6/10;

+ Mức độ: Critical;

+ Lỗ hổng này xảy ra do đường dẫn tìm kiếm không đáng tin cậy trong một số ứng dụng Zoom Client dành cho Windows có thể cho phép người dùng chưa xác thực thực hiện hành vi leo thang đặc quyền thông qua quyền truy cập mạng. Bằng cách đặt tệp độc hại vào vị trí được tìm kiếm trước đường dẫn tệp hợp lệ, tin tặc có thể thông qua chia sẻ mạng lừa ứng dụng thực thi mã độc hại với đặc quyền cao hơn.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng tới các phiên bản:

+ Zoom Workplace dành cho Windows trước phiên bản 6.3.10.

+ Zoom Workplace VDI dành cho Windows trước phiên bản 6.3.10 (ngoại trừ 6.1.16 va 6.2.12).

+ Zoom Rooms dành cho Windows trước phiên bản 6.3.10.

+ Bộ điều khiển Zoom Rooms dành cho Windows trước phiên bản 6.3.10.

+ Zoom Meeting SDK dành cho Windows trước phiên bản 6.3.10.

- Khuyến nghị: Zoom đã phát hành bản cập nhật bảo mật để giải quyết lỗ hổng này. Người dùng được khuyến cáo nên cập nhật ngay lập tức ứng dụng Zoom lên phiên bản 6.3.10 trở lên thông qua Trung tâm Tải xuống Zoom chính thức. Đối với môi trường VDI, phiên bản 6.1.16 và 6.2.12 cũng bao gồm bản sửa lỗi: https://www.zoom.com/en/trust/security-bulletin/zsb-25030.

- 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 hỗ trợ.

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