BỘ CÔNG AN
CÔNG AN TỈNH QUẢNG NGÃI

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

Số: 3438 /CAT-ANM
V/v cảnh báo lỗ hổng bảo mật nghiêm trọng tháng 10/2025

Quảng Ngãi, ngày 04 tháng 11 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 10/2025, 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 07 lỗ hổng bảo mật có mức độ rất nghiêm trọng, 03 lỗ hổng bảo mật nghiêm trọng, 01 lỗ hổng bảo mật mức trung bình; 05 lỗ hổng đã công khai POC, cụ thể:

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

1.1. CVE-2025-55241 *– Lỗ hổng nâng cao đặc quyền trong Microsoft Entra ID (trước đây là Azure Active Directory)*

- Mô tả:

+ Điểm CVSS: 10/10;

+ Mức độ: Critical;

+ Lỗ hổng này phát sinh từ vấn đề không xác thực đối tượng giữa dịch vụ kiểm soát truy cập ASC của Microsoft và Azure AD Graph API cũ, cho phép sử dụng mã thông báo để truy cập giữa các tài khoản. Tin tặc khi khai thác lỗ hổng thành công có thể truy cập thông tin người dùng được lưu trữ trong Entra ID, chi tiết nhóm và vai trò, cài đặt đối tượng thuê, quyền ứng dụng, thông tin thiết bị và khóa BitLocker được đồng bộ hóa với Entra ID mà không để lại bất kỳ dấu vết nào.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hướng đến tất cả phiên bản Azure AD Graph.

- Khuyến nghị: Microsoft đã xác nhận lỗ hổng và khuyến cáo quản trị viên nên đảm bảo các bên thuê của mình đã nhận được bản cập nhật của Microsoft và xóa hoặc thay thế bất kỳ phần phụ thuộc nào còn lại trên Azure AD Graph bảng Microsoft Graph. Ngoài ra, không cần thực hiện thêm hành động nào. Thông tin chi tiết bản cập nhật: https://msrc.microsoft.com/update-guide/vulnerabilitv/CVE-2025-55241.

- Lỗ hổng chưa có PoC công khai.

1.2. CVE-2025-59230 *– Lỗ hổng nâng cao đặc quyền của Windows Remote Access Connection Manager.*

- Mô tả:

+ Điểm CVSS: 7.8/10;

+ Mức độ: High;

+ Lỗ hổng kiểm soát truy cập không đúng cách trong Windows Remote Access Connection Manager - dịch vụ cốt lõi của Windows giúp quản lý các kết nối quay số và Mạng riêng ảo (VPN), cho phép máy tính của bạn kết nối an toàn với các mạng từ xa. Cho phép tin tặc nâng cao đặc quyền cục bộ. Khi khai thác thành công lỗ hổng, tin tặc có thể giành được đặc quyền hệ thống.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hường đến Windows 10 Version 1809 từ 10.0.17763.0 đến trước 10.1.17763.7919. Windows 11 version 22H2 từ 10.0.22621 0 đến trước 10.0.22621.6060.

- Khuyến nghị: Microsoft khuyến cáo người dùng nên áp dụng bản vá do Microsoft phát hành, nếu chưa thể cập nhật có thể làm các bước:

+ Hạn chế ACL dịch vụ RasMan: Sử dụng sc sdset RasMan để thực thi DACL.

+ Bật Credential Guard và Protected Process Light cho các dịch vụ quan trọng.

+ Triển khai AppLocker hoặc WDAC để chặn các tệp thực thi chưa được ký.

Thông tin chi tiết: https://msrc.microsoft.com/update-guide/vulnerability/CVE- 2025-59230.

- Lỗ hổng có PoC: https://github.com/moegameka/CVE-2025-5923Q.

1.3. CVE-2025-55315 *– Lỗ hổng bỏ qua tính năng bảo mật trong ASP.NET*

- Mô tả:

+ Điểm CVSS: 9.9/10;

+ Mức độ: Critical;

+ Tin tặc khai thác lỗ hổng có thể lạm dụng để âm thầm vượt qua các biện pháp kiểm soát bảo mật và thực hiện các hành động độc hại bằng cách lén lút đưa một yêu cầu HTTP thứ hai vào nội dung của yêu cầu được xác thực ban đầu.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến các phiên bản ASP.NET Core trước 10.0.0-rc.1.25451.107, ASP.NET Core trước 9.0.9, ASP.NET Core trước 8.0.20 và ASP.NET Core 2.X sử dụng gói Microsoft.AspNetCore.Server.Kestrel.Core phiên bản 2.3.0 trở về trước.

- Khuyến nghị: Microsoft khuyến cáo người dùng đảm bảo an toàn cho ứng dụng ASP.NET bằng cách:

+ Nếu đang chạy .NET 8 trở lên, hãy cài đặt bản cập nhật .NET từ Microsoft Update, sau đó khởi động lại ứng dụng hoặc khởi động lại máy.

+ Nếu đang chạy .NET 2.3, bạn phải cập nhật tham chiếu gói cho Microsoft.AspNet.Server.Kestrel.Core lên 2.3.6, sau đó biên dịch lại ứng dụng và triển khai lại.

+ Nếu đang chạy một ứng dụng độc lập/tệp đơn, hãy cài đặt bản cập nhật .NET, biên dịch lại ứng dụng và triển khai lại.

Thông tin chi tiết: https://msrc.microsoft.com/update-guide/vulnerability/CVE- 2025-55315.

- Lỗ hổng có PoC: https://github.com/nickcopi/CVE-2025-55315-detection- playground.

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

CVE-2025-32463 *– Lỗ hổng chạy lệnh tùy ý dưới quyền Root trong tiện ích Sudo*

- Mô tả

+ Điểm CVSS: 9.3/10;

+ Mức độ: Critial;

+ Lỗ hổng này cho phép tin tặc leo thang đặc quyền bằng cách lừa Sudo tải một thư viện dùng chung tùy ý bằng thư mục gốc do người dùng chỉ định thông qua tùy chọn -R(--chroot). Tin tặc có thể chạy các lệnh tùy ý với tư cách root trên các hệ thống hỗ trợ /etc/nsswitch.conf.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến các phiên bản Sudo từ 1.9.14 đến trước phiên bản 1.9.17p1.

- Khuyến nghị: Nhà phát hành khuyến cáo người dùng cài đặt phiên bản sudo mới nhất. Trường hợp không thể cài đặt phiên bản mới nên tránh sử dụng tùy chọn chroot, vì điều này có thể vô tình làm giảm tính bảo mật của môi trường nếu không được triển khai đúng cách. Truy cập https://www.sudo.ws/securitv/advisories/chroot_bug/ để biết thêm thông tin chi tiết.

- Lỗ hổng có PoC: https://github.com/pr0v3rbs/CVE-2025-32463_chwoot.

3. Lỗ hổng bảo mật phần mềm trên tường lửa

CVE-2025-20363 *– Lỗ hổng RCE trong các ứng dụng tường lửa bảo mật của Cisco*

- Mô tả:

+ Điểm CVSS: 9/10;

+ Mức độ: Critial;

+ Lỗ hổng này xuất phát từ việc xác thực không đúng dữ liệu đầu vào do người dùng cung cấp trong các yêu cầu HTTP. Tin tặc có thể khai thác lỗ hổng này bằng cách gửi các yêu cầu HTTP được tạo sẵn đến một dịch vụ web mục tiêu trên thiết bị bị ảnh hưởng sau khi thu thập thêm thông tin về hệ thống, vượt qua các biện pháp giảm thiểu khai thác, hoặc cả hai. Khi khai thác thành công có thể cho phép tin tặc thực thi mã tùy ý dưới quyền root, điều này có thể dẫn đến việc chiếm quyền điều khiển hoàn toàn thiết bị bị ảnh hưởng.

- Phiên bản ảnh hưởng: Lỗ hổng này ảnh hưởng các ứng dụng Secure Firewall ASA, Secure Firewall Threat Defense FTD.

- Khuyến nghị: Cisco đã phát hành bản cập nhật phần mềm để giải quyết lỗ hổng này và khuyến nghị khách hàng nên nâng cấp lên bản vá lỗi. Trong trường hợp chưa thể cập nhật, quản trị viên có thể giảm thiểu rủi ro bằng cách vô hiệu hóa tất cả các dịch vụ web VPN dựa trên SSL/TLS, chẳng hạn như vô hiệu hóa dịch vụ máy khách IKEv2 và vô hiệu hóa tất cả các dịch vụ VPN SSL.

Để biết thêm chi tiết: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-http-code-exec-WmfP3h30.

- Lỗ hổng chưa có PoC công khai

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

4.1. CVE-2025-62168 *– Lỗ hổng rò rỉ thông tin xác thực HTTP trong dịch vụ tăng tốc lưu lượng web Proxy Squid.*

- Mô tả:

+ Điểm CVSS: 10/10;

+Mức độ: Critial;

+ Lỗ hổng này phát sinh do lỗi không biên tập thông tin xác thực HTTP trong quá trình xử lý lỗi, có khả năng cho phép tin tặc vượt qua các biện pháp bảo mật của trình duyệt và thu thập mã thông báo xác thực hoặc thông tin xác thực nhạy cảm được sử dụng bởi các máy khách và ứng dụng phụ trợ đáng tin cậy.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến các phiên bản Proxy Squid từ 7.1 trở xuống.

- Khuyến nghị: Nhà phát hành thông báo lỗ hổng đã được giải quyết hoàn toàn trong Proxy Squid phiên bản 7.2, phiên bản này triển khai tính năng biên tập thông tin xác thực mạnh mẽ trong tất cả các chức năng xử lý lỗi. Ngoài ra nhà phát hành cũng cung cấp các bản vá trực tiếp cho người dùng không thể nâng cấp ngay lập tức, thông tin bản vá: https://github.com/squid-Cache/squid/commit/0951a0681011dfca3d78c84fd7f1e19c78a4443f.

- Lỗ hổng chưa có PoC công khai.

4.2. CVE-2025-59681 *– Lỗ hổng SQL Injection nghiêm trọng trong python Django.*

- Mô tả:

+ Điểm CVSS: 9.8/10;

+ Mức độ: Critial;

+ Lỗ hổng này xảy ra khi sử dụng một từ điển được thiết kế phù hợp với phần mở rộng từ điển là **kwargs được truyền đến các phương thức QuerySet bị ảnh hưởng (annotate(), alias(), aggregate() và extra()) cụ thể trên cơ sở dữ liệu MySQL và MariaDB. Tin tặc khi khai thác thành công có thể thao túng các truy vấn SQL, có khả năng dẫn đến rò rỉ dữ liệu hoặc làm hỏng dữ liệu trong các ứng dụng Django chạy trên cơ sở dữ liệu bị ảnh hưởng.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến Django phiên bản 4.2 đến trước 4.2.25, từ 5.1 đến trước 5.1.13 và từ 5.2 đến trước 5.2.7.

- Khuyến nghị: Nhà phát hành Django đã công bố bản vá cho tất cả các phiên bản bị ảnh hưởng: Django 4.2.25, Django 5.1.13 và Django 5.2.7. Người dùng được khuyến khích nâng cấp lên các phiên bản vá lỗi này ngay lập tức. Các bản sửa lỗi đã được áp dụng cho nhánh chính của Django, 6.0 (trạng thái alpha), 5.2, 5.1 và 4.2. Thông tin chi tiết bản cập nhật: https://www.djangoproject.com/weblog/2025/oct/01/security-releases/.

- Lỗ hổng chưa có PoC công khai.

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

CVE-2025-59689 *– Lỗ hổng chèn lệnh từ xa Libraesva Email Security Gateway.*

- Mô tả:

+ Điểm **CVSS:** 6.1/10;

+ Mức độ: Medium;

+ Tin tặc có thể khai thác lỗ hổng bằng cách chèn lệnh có thể được kích hoạt bởi một email chứa tệp đính kèm nén được thiết kế đặc biệt, cho phép thực thi các lệnh tùy ý với tư cách là người dùng không có đặc quyền. Điều này xảy ra do quá trình quét file không đúng cách trong quá trình xóa mã thực thi khỏi các tệp trong một số định dạng lưu trữ nén.

- Phiên bản ảnh hưởng: Lỗ hổng bảo mật này ảnh hưởng đến các phiên bản Libraesva ESG bắt đầu từ phiên bản 4.5 đến trước phiên bản 5.0.31.

- Khuyến nghị: Libraesva đã phát hành bản vá khẩn cấp, tự động cho tất cả khách hàng cài đặt ESG 5.x và không cần thực hiện thao tác nào khác. Đối với các khách hàng đang sử dụng phiên bản 4.x cần cập nhật thủ công theo hướng dẫn chi tiết sau đây: https://docs.libraesva.com/document/migration/libraesva-esq-4-x-to-5-x-migration-guide/.

- Lỗ hổng chưa có PoC công khai.

6. Lỗ hổng bảo mật phần mềm trên trình duyệt

CVE-2025-11152 *– Lỗ hổng tràn số nguyên gây thoát khỏi Sandbox trên Firefox.*

- Mô tả:

+ Điểm CVSS: 8.6/10;

+ Mức độ: High;

+ Lỗ hổng này cho phép thoát khỏi sandbox thông qua lỗi tràn số nguyên trong thành phần Graphics: Canvas2D, có thể dẫn đến các hệ quả bảo mật nghiêm trọng như truy cập dữ liệu nhạy cảm từ bộ nhớ, có thể đọc/ghi vùng nhớ khác (memory corruption), dẫn tới tiết lộ dữ liệu hoặc thực thi mã độc.

+ Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến các phiên bản Firefox 143.0.3 trở xuống.

- Khuyến nghị: Mozilla đã khắc phục lỗ hổng này trong Firefox phiên bản 143.0.3. Người dùng được khuyến cáo nên cập nhật lên phiên bản này hoặc phiên bản mới hơn để giảm thiểu rủi ro. Bản sửa lỗi đã được tích hợp vào nhiều bản phân phối Linux, trong đó Ubuntu và Debian đã cung cấp các gói cập nhật. Chi tiết bản cập nhật: https://www.mozilla.org/en-US/security/advisories/mfsa2025-80/.

- Lỗ hổng chưa có PoC công khai.

7. Lỗ hổng bảo mật khác

7.1. CVE-2025-41244 *– Lỗ hổng leo thang đặc quyền cục bộ trên Vmware Aria Operations và VMware Tools.*

- Mô tả:

+ Điểm CVSS: 7.8/10;

+ Mức độ: High;

+ Tin tặc không có quyền phải quản trị viên trên Máy ảo (VM) khách có thể khai thác lỗ hổng này để chiếm quyền root trên VM. Vấn đề nằm ở logic của plugin service-discovery, có thể thực thi các tệp nhị phân do tin tặc kiểm soát từ các đường dẫn có thể ghi như /tmp. Việc khai thác yêu cầu phải cài đặt gói open-vm-tools-sdmp và bật tính năng guest service discovery.

- Phiên bản ảnh hưởng: Lỗ hổng bảo mật này ảnh hưởng đến các phiên bản:

+ VMware Cloud Foundation 4.x và 5.x;

+ VMware Cloud Foundation 9.xxx;

+ VMware Cloud Foundation 13.xxx (Windows, Linux);

+ VMware vSphere Foundation 9.xxx;

+ VMware vSphere Foundation 13.xxx (Windows, Linux);

+ VMware Aria Operations 8.x;

+ VMware Tools 11.xx, 12.xx và 13.xx (Windows, Linux);

+ Nền tảng đám mây viên thông VMware 4.x và 5.x;

+ Cơ sở hạ tầng đám mây viên thông VMware 2.x và 3.x.

- Khuyến nghị: Có hai cách chính để loại bỏ nguy cơ lỗ hổng bảo mật này:

+ Tạm thời - Vô hiệu hóa các tính năng khám phá dịch vụ khách: Vô hiệu hóa plugin servicediscovery trong cấu hình hoặc bằng cách chạy lệnh 'vmware-toolbox-cmd config set servicediscovery disabled true' rồi khởi động lại hệ thống.

+ Vĩnh viễn - Gỡ cài đặt 'open-vm-tools-sdmp' rồi khởi động lại hệ thống.

- Lỗ hổng có PoC: https://github.com/rxerium/CVE-2025-41244.

7.2. CVE-2025-11001 *– Lỗ hổng cho phép thực thi mã từ xa trong 7-Zip.*

- Mô tả:

+ Điểm CVSS: 9.8/10;

+ Mức độ: Critial;

+ Lỗ hổng này cho phép tin tặc tạo ra các tệp ZIP độc hại, khi được giải nén bằng các phiên bản 7-Zip dễ bị tấn công, có thể ghi các tệp ra ngoài thư mục giải nén. Lỗ hổng chỉ có thể bị khai thác khi 7-Zip được chạy với quyền Quản trị viên.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng tới các phiên bản 7-Zip từ 21.02 đến 25.00.

- Khuyến nghị: Nhà phát hành thông báo lỗ hổng đã được khắc phục trong phiên bản 7-Zip V25.00. Người dùng được khuyến nghị nên nâng cấp lên phiên bản mới nhất ngay lập tức do phần mềm không tự động cập nhật. Chi tiết hướng dẫn cập nhật: https://www.7- zip.org/download.html.

- Lỗ hổng có PoC: https://github.com/shalevo13/Se7enSlip

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