BỘ CÔNG AN
CÔNG AN TỈNH ĐỒNG THÁP

Số:6545 /CAT-ANM

V/v cảnh báo một số lỗ hổng nguy hiểm đã được công bố tháng 6 năm 2026

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

Đồng Tháp, ngày 17 tháng 07 năm 2026

Kính gửi:
- Các sở, ban, ngành, đơn vị sự nghiệp, doanh nghiệp nhà nước thuộc tỉnh;
- Ủy ban nhân dân các xã, phường.

Thời gian qua, nhiều lỗ hổng, nguy cơ bảo mật được phát hiện, công bố có khả năng bị các tin tặc khai thác, tấn công vào hệ thống thông tin cơ quan, tổ chức nhà nước, doanh nghiệp, cụ thể:

- **Lỗ hổng leo thang đặc quyền trong ASP.NET Core CVE-2026-40372 -** Lỗ hổng trong Microsoft.AspNetCore.

- **Lỗ hổng giả mạo máy chủ Microsoft SharePoint CVE-2026-32201 -** Lỗ hổng nằm ở cơ chế xử lý yêu cầu của SharePoint.

- **Lỗ hổng leo thang đặc quyền trong Microsoft Defender CVE-2026-33825 -** Lỗ hổng bắt nguồn từ tình trạng tranh chấp trong logic sửa chữa tập tin của Windows Defender.

- **Lỗ hổng Pack2TheRoot mới cho phép truy cập quyền root vào Linux CVE-2026-41651 -** Lỗ hổng được phát hiện trong PackageKit.

- **Lỗ hổng gây vô hiệu hóa các biện pháp bảo vệ trên tường lửa SonicWall CVE-2026-0204 -** Lỗ hổng trong cơ chế kiểm soát truy cập của SonicOS.

- **Lỗ hổng file upload trong plugin Breeze Cache của WordPress CVE-2026-3844 -** Lỗ hổng này bắt nguồn từ việc thiếu xác thực loại tệp trong hàm 'fetch_gravatar_from_remote'.

- **Lỗ hổng XSS trên Microsoft Exchange cho phép xâm nhập vào hộp thư Outlook Web Access (OWA) CVE-2026-42897 -** Lỗ hổng bắt nguồn từ lỗi kịch bản chéo trang (XSS).

- **Lỗ hổng chèn lệnh trong framework SGLang cho phép thực thi mã từ xa CVE-2026-5760 -** Lỗ hổng xuất phát từ cách hệ thống xử lý template.

- **Lỗ hổng tràn số nguyên trong Blink trên Chromium CVE-2026-7896 -** Lỗ hổng xảy ra do lỗi tràn số nguyên trong Blink của Google Chrome.

- **Lỗ hổng thực thi mã từ xa trên GitHub.com và GitHub Enterprise Server CVE-2026-3854 -** Lỗ hổng do vấn đề chèn lệnh gây ra, cho phép tin tặc có quyền truy cập đẩy (push) vào kho lưu trữ thực hiện thực thi mã từ xa.

- Lỗ hổng thực thi mã từ xa trên hệ điều hành Android CVE-2026-0073

- Lỗ hổng xảy ra do lỗi logic trong hàm adbd_tls_verify_cert của thành phần con auth.cpp trong trình nền ADB (adbd).

Tình hình trên, Công an tỉnh đề nghị quý cơ quan, đơn vị chủ động rà soát trên hệ thống thông tin do cơ quan, đơn vị mình quản lý, vận hành để phòng ngừa, kịp thời cập nhật bản vá. Khi phát sinh tình hình có liên quan, kịp thời trao đổi về Công an tỉnh (qua Phòng an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, số điện thoại 0693.599.332) để phối hợp xử lý (gửi kèm phụ lục chi tiết các lỗ hổng và các biện pháp phòng ngừa)./.

Nơi nhận:
- Như trên;
- Đ/c Giám đốc CAT (để báo cáo);
- Phòng ANM&PCTPSDCNC (để thực hiện);
- Phòng Tham mưu (để nắm);
- Lưu CAT: VT, AMN(Đ4).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
CÔNG AN TỈNH ĐỒNG THÁP

Đại tá Nguyễn Minh Tân

PHỤ LỤC

(Kèm theo Công văn số: /CAT-ANM, ngày / /2026 của Công an tỉnh)

1. Lỗ hổng leo thang đặc quyền trong ASP.NET Core CVE-2026-40372 - Lỗ hổng trong Microsoft.AspNetCore.

a) Mô tả

- Điểm CVSS: 9.1/10;

- Mức độ: Critical;

- Lỗ hổng trong Microsoft.AspNetCore. DataProtection cho phép tin tặc sử dụng các payload giả mạo để xác thực với tư cách người dùng có đặc quyền có thể khiến ứng dụng tự động cấp cho mình các token được ký hợp lệ (làm mới phiên, khóa API, liên kết đặt lại mật khẩu, v.v.). Từ cookie giả mạo đó, tin tặc có thể thực hiện tấn công nâng cao đặc quyền, đồng thời cho phép giải mã một số payload được bảo vệ.

- Lỗ hổng ảnh hưởng đến các phiên bản ASP.NET Core từ 10.0.0 đến 10.0.6.

b) Kiến nghị

Microsoft đã phát hành bản cập nhật ngoài luồng để khắc phục lỗ hổng bảo mật trong phiên bản ASP.NET Core 10.0.7. Người dùng nên cập nhật sớm nhất có thể, thao tác này sẽ khắc phục lỗ hổng trong quy trình xác thực. Bất kỳ payload giả mạo nào được tạo sẽ bị mã đã sửa lỗi từ chối. Thông tin chi tiết:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40372.

2. Lỗ hổng giả mạo máy chủ Microsoft SharePoint CVE-2026-32201 - Lỗ hổng nằm ở cơ chế xử lý yêu cầu của SharePoint.

a) Mô tả

- Điểm CVSS: 6.5/10;

- Mức độ: Medium;

- Lỗ hổng nằm ở cơ chế xử lý yêu cầu của SharePoint. Do việc xác thực dữ liệu đầu vào do người dùng cung cấp không đầy đủ, tin tặc không cần xác thực có thể thao túng các tham số yêu cầu HTTP để vượt qua các biện pháp kiểm soát bảo mật.

- Lỗ hổng ảnh hưởng đến các phiên bản SharePoint Server 2016, SharePoint Server 2019, SharePoint Server Subscription Edition.

b) Kiến nghị

Microsoft đã phát hành bản cập nhật bảo mật đối với lỗ hổng này. Trường hợp chưa thể áp dụng bản vá, người dùng có thể hạn chế truy cập từ bên ngoài vào các phiên bản SharePoint thông qua VPN hoặc Truy cập mạng không tin cậy. Hoặc cấu hình các quy tắc Tường lửa ứng dụng web (WAF) để lọc và chặn các cấu trúc yêu cầu HTTP đáng ngờ. Thông tin chi tiết:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32201.

3. Lỗ hổng leo thang đặc quyền trong Microsoft Defender CVE-2026-33825 - Lỗ hổng bắt nguồn từ tình trạng tranh chấp trong logic sửa chữa tập tin của Windows Defender.

a) Mô tả

- Điểm CVSS: 7.8/10;

- Mức độ: High;

- Lỗ hổng bắt nguồn từ tình trạng tranh chấp trong logic sửa chữa tập tin của Windows Defender, có thể bị khai thác để ghi đè lên các tập tin tùy ý trên hệ thống. Khai thác thành công cho phép tin tặc đạt được quyền thực thi mã cấp SYSTEM từ một tài khoản không có đặc quyền.

- Lỗ hổng ảnh hưởng đến tất cả phiên bản Windows 10, Windows 11, Windows Server 2016, 2019, 2022, 2025.

b) Kiến nghị

Microsoft đã phát hành bản cập nhật bảo mật Patch Tuesday tháng 4 năm 2026 khắc phục sự cố. Các tổ chức được khuyến cáo mạnh mẽ nên áp dụng ngay lập tức. Thông tin chi tiết: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33825.

4. Lỗ hổng Pack2TheRoot mới cho phép truy cập quyền root vào Linux CVE-2026-41651 - Lỗ hổng được phát hiện trong PackageKit.

a) Mô tả

- Điểm CVSS: 8.8/10;

- Mức độ: High;

- Lỗ hổng được phát hiện trong PackageKit, xảy ra do tình trạng tranh chấp thời điểm kiểm tra và thời điểm sử dụng (TOCTOU) trên các cờ giao dịch cho phép người dùng không có đặc quyền cài đặt các gói với quyền root, dẫn đến leo thang đặc quyền cục bộ. Để khai thác lỗ hổng này, tin tặc cần có quyền truy cập cục bộ vào hệ thống và các quyền cơ bản để cài đặt gói thông qua PackageKit, do đó chỉ những người dùng đã xác thực mới có thể tiếp cận được.

- Lỗ hổng ảnh hưởng đến các phiên bản PackageKit từ 1.0.2 đến 1.3.4.

b) Kiến nghị

Nhà phát hành thông báo lỗ hổng này đã được vá trong phiên bản 1.3.5, người dùng nên áp dụng bản vá sớm nhất có thể. Trường hợp chưa thể áp dụng bản vá có thể giảm thiểu lỗ hổng bằng cách ẩn dịch vụ PackageKit. Lưu ý rằng các trình quản lý gói đồ họa, chẳng hạn như phần mềm GNOME, sẽ không hoạt động như mong đợi cho đến khi dịch vụ được bỏ ẩn.

5. Lỗ hổng gây vô hiệu hóa các biện pháp bảo vệ trên tường lửa SonicWall CVE-2026-0204 - Lỗ hổng trong cơ chế kiểm soát truy cập của SonicOS.

a) Mô tả

- Điểm CVSS: 8.0/10;

- Mức độ: High;

- Lỗ hổng trong cơ chế kiểm soát truy cập của SonicOS có thể cho phép truy cập vào một số chức năng giao diện quản lý nhất định trong những điều kiện cụ thể. Tin tặc có quyền truy cập vào giao diện quản trị có thể thay đổi cấu hình tường lửa và vô hiệu hóa các biện pháp bảo vệ an ninh.

- Lỗ hổng này ảnh hưởng đến các trường lửa đang chạy các phiên bản firmware lên đến 6.5.5.1-6n, 7.0.1-5169, 7.3.1-7013 và 8.1.0-8017.

b) Kiến nghị

Nhà phát hành thông báo các bản vá lỗi đã được bao gồm trong các bản phát hành firmware 6.5.5.2-28n, 7.3.2-7010 và 8.2.0-8009, và khách hàng được khuyến cáo nên cập nhật thiết bị của mình càng sớm càng tốt, hoặc hạn chế quyền truy cập quản lý chỉ qua SSH cho đến khi có thể vá lỗi, bằng cách vô hiệu hóa quản lý dựa trên HTTP/HTTPS và SSLVPN trên tất cả các giao diện. Thông tin chi tiết: https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0004.

6. Lỗ hổng file upload trong plugin Breeze Cache của WordPress CVE-2026-3844 - Lỗ hổng này bắt nguồn từ việc thiếu xác thực loại tệp trong hàm 'fetch_gravatar_from_remote'.

a) Mô tả

- Điểm CVSS: 9.8/10;

- Mức độ: Critical;

- Lỗ hổng này bắt nguồn từ việc thiếu xác thực loại tệp trong hàm 'fetch_gravatar_from_remote', cho phép tin tặc không được xác thực tải lên các tệp tùy ý. Điều này có thể dẫn đến thực thi mã từ xa và chiếm quyền kiểm soát toàn bộ trang web. Việc khai thác chỉ có thể thực hiện được nếu tùy chọn "Lưu trữ tệp cục bộ - Gravatar" được bật.

- Lỗ hổng ảnh hưởng đến các phiên bản Breeze Cache WordPress từ 2.4.4 trở xuống.

b) Kiến nghị

Nhà phát hành thông báo lỗ hổng đã được khắc phục trong phiên bản 2.4.5. Người dùng Breeze Cache nên cập nhật lên phiên bản mới nhất ngay lập tức hoặc tạm thời vô hiệu hóa plugin. Thông tin chi tiết: https://github.com/dinosn/CVE-2026-3844.

7. Lỗ hổng XSS trên Microsoft Exchange cho phép xâm nhập vào hộp thư Outlook Web Access (OWA) CVE-2026-42897 - Lỗ hổng bắt nguồn từ lỗi kịch bản chéo trang (XSS).

a) Mô tả

- Điểm CVSS: 8.1/10;

- Mức độ: High;

- Lỗ hổng này bắt nguồn từ lỗi kịch bản chéo trang (XSS). Tin tặc có thể khai thác lỗ hổng này bằng cách gửi một email được soạn thảo đặc biệt cho người dùng. Nếu người dùng mở email đó trong Outlook Web Access và đáp ứng một số điều kiện tương tác nhất định, mã JavaScript tùy ý có thể được thực thi trong ngữ cảnh trình duyệt.

- Lỗ hổng này ảnh hưởng đến các phiên bản Exchange Server 2016, Exchange Server 2019 và Exchange Server Subscription Edition (SE).

b) Kiến nghị

Microsoft thông báo đã cung cấp hai tùy chọn khắc phục sự cố mà khách hàng có thể áp dụng trong khi chờ bản vá lỗi. Tùy chọn đầu tiên, được Microsoft khuyến nghị, dành cho các tổ chức sử dụng Dịch vụ Khắc phục Sự cố Khẩn cấp Exchange (EM), dịch vụ này đã nhận được bản vá lỗi cho các phiên bản Exchange Server 2016, 2019 và SE được kích hoạt tự động. Phương án giảm thiểu rủi ro thứ hai là sử dụng công cụ Exchange On-premises Mitigation Tool (EOMT) được cập nhật, mà Microsoft khuyến nghị khách hàng nên tải xuống và áp dụng cho từng máy chủ hoặc bằng cách thực thi tập lệnh thông qua Exchange Management Shell (EMS) với quyền quản trị viên.

8. Lỗ hổng chèn lệnh trong framework SGLang cho phép thực thi mã từ xa CVE-2026-5760 - Lỗ hổng xuất phát từ cách hệ thống xử lý template.

a) Mô tả

- Điểm CVSS: 9.8/10;

- Mức độ: Critical;

- Lỗ hổng xuất phát từ cách hệ thống xử lý template. SGLang sử dụng Jinja2 để render nội dung từ các file model, nhưng lại không áp dụng cơ chế sandbox an toàn. Thay vào đó, hệ thống sử dụng môi trường mặc định "jinja2.Environment()" cho phép thực thi mã Python. Tin tặc có thể chèn payload vào tham số tokenizer.chat_template bên trong file mô hình định dạng GGUF. Khi tệp này được tải lên hệ thống, payload sẽ không được thực thi ngay lập tức mà chờ cho đến khi endpoint /v1/rerank được gọi.

- Lỗ hổng ảnh hưởng đến tất cả các phiên bản framework SGLang.

b) Kiến nghị

Nhà phát hành hiện nay chưa đưa ra bản vá phù hợp, khuyến cáo người dùng sử dụng ImmutableSandboxedEnvironment thay vì jinja2.Environment() để hiển thị các mẫu trò chuyện. Điều này sẽ ngăn chặn việc thực thi mã Python tùy ý trên máy chủ. Thông tin chi tiết: https://www.kb.cert.org/vuls/id/915947.

9. Lỗ hổng tràn số nguyên trong Blink trên Chromium CVE-2026-7896 - Lỗ hổng xảy ra do lỗi tràn số nguyên trong Blink của Google Chrome.

a) Mô tả

- Điểm CVSS: 8.8/10;

- Mức độ: High;

- Lỗ hổng xảy ra do lỗi tràn số nguyên trong Blink của Google Chrome, cho phép tin tặc tấn công từ xa có khả năng khai thác lỗ hổng bộ nhớ heap thông qua một trang HTML được tạo sẵn.

- Lỗ hổng ảnh hưởng đến Google Chrome phiên bản trước 148.0.7778.96 (Linux); Google Chrome phiên bản trước 148.0.7778.96/97 (Mac); Google Chrome phiên bản trước 148.0.7778.96/97 (Windows).

b) Kiến nghị

Google thông báo các bản vá lỗi cho lỗ hổng bảo mật này đã được tích hợp trong các phiên bản Chrome 148.0.7778.96. Người dùng nên cập nhật trình duyệt của mình càng sớm càng tốt, vì các lỗ hổng bảo mật của Chrome thường là mục

tiêu của các cuộc tấn công. Thông tin chi tiết: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-7896.

10. Lỗ hổng thực thi mã từ xa trên GitHub.com và GitHub Enterprise Server CVE-2026-3854 - Lỗ hổng do vấn đề chèn lệnh gây ra, cho phép tin tặc có quyền truy cập đẩy (push) vào kho lưu trữ thực hiện thực thi mã từ xa.

a) Mô tả

- Điểm CVSS: 8.8/10;

- Mức độ: High;

- Lỗ hổng này do vấn đề chèn lệnh gây ra, cho phép tin tặc có quyền truy cập đẩy (push) vào kho lưu trữ thực hiện thực thi mã từ xa trên máy chủ đó. Trong quá trình thực hiện thao tác git push, các giá trị tùy chọn push không được xử lý đúng cách trước khi được đưa vào tiêu đề dịch vụ nội bộ. Vì định dạng tiêu đề nội bộ sử dụng ký tự phân cách cũng có thể xuất hiện trong dữ liệu đầu vào của người dùng, tin tặc có thể chèn thêm các trường siêu dữ liệu thông qua các giá trị tùy chọn push được tạo sẵn.

- Lỗ hổng bảo mật này ảnh hưởng đến các phiên bản các phiên bản Enterprise Server trước 3.19.1.

b) Kiến nghị

GitHub nhanh chóng khắc phục sự cố bằng cách làm sạch dữ liệu đầu vào và phát hành các bản vá cho các phiên bản Enterprise Server. Người dùng GitHub.com không cần thực hiện bất kỳ hành động nào.

11. Lỗ hổng thực thi mã từ xa trên hệ điều hành Android CVE-2026-0073 - Lỗ hổng xảy ra do lỗi logic trong hàm adbd_tls_verify_cert của thành phần con auth.cpp trong trình nền ADB (adbd).

a) Mô tả

- Điểm CVSS: 8.8/10;

- Mức độ: High;

- Lỗ hổng xảy ra do lỗi logic trong hàm adbd_tls_verify_cert của thành phần con auth.cpp trong trình nền ADB (adbd). Tin tặc có quyền truy cập mạng lân cận có thể khai thác lỗ hổng này để thực hiện thực thi mã từ xa (RCE) với tư cách người dùng shell. Việc khai thác này không yêu cầu đặc quyền bổ sung và không cần tương tác của người dùng.

- Lỗ hổng bảo mật này ảnh hưởng đến các phiên bản Android 14 trước bản vá bảo mật ngày 01/05/2026; Android 15 trước bản vá bảo mật ngày 01/05/2026; Android 16 trước bản vá bảo mật ngày 01/05/2026; Android 16-qpr2 trước bản vá bảo mật ngày 01/05/2026.

b) Kiến nghị

Nhà phát hành thông báo đã phát hành các bản vá mã nguồn tương ứng cho kho lưu trữ Dự án nguồn mở Android (AOSP). Người dùng cần nâng cấp các hệ thống bị ảnh hưởng lên bản vá bảo mật ngày 01/05/2026 trở lên. Thông tin chi tiết: https://source.android.com/docs/security/bulletin/2026/2026-05-01?hl=vi./.