

**BỘ CÔNG AN
CÔNG AN TỈNH ĐỒNG THÁP**

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

Số: 8229/CAT-ANM

Đồng Tháp, ngày 16 tháng 09 năm 2026

V/v cảnh báo một số lỗ hổng nguy hiểm
đã được công bố tháng 8 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 thực thi mã từ xa trong Microsoft SharePoint Server - CVE-2026-50522** - Lỗ hổng phát sinh từ cơ chế xử lý dữ liệu không an toàn trong Microsoft SharePoint Server.

- **Lỗ hổng thực thi mã từ xa trong Windows IKE Extension - CVE-2026-33824** - Lỗ hổng phát sinh từ lỗi giải phóng bộ nhớ hai lần trong thành phần Windows IKE Extension.

- **Lỗ hổng leo thang đặc quyền trong Windows Ancillary Function Driver for WinSock - CVE-2026-68820** - Lỗ hổng phát sinh từ lỗi giải phóng bộ nhớ nhưng vẫn tiếp tục sử dụng trong trình điều khiển AFD.sys (Windows Ancillary Function Driver for WinSock).

- **Lỗ hổng leo thang đặc quyền trong Windows User Profile Service - CVE-2026-62832** - Lỗ hổng phát sinh do cơ chế xử lý liên kết (symlink/junction) trước khi truy cập tệp không phù hợp trong dịch vụ Windows User Profile Service.

- **Lỗ hổng giả mạo dữ liệu trong Windows Container Isolation FS Filter Driver - CVE-2026-72971** - Lỗ hổng liên quan đến cơ chế xử lý liên kết tệp trong trình điều khiển unionfs.sys (Windows Container Isolation FS Filter Driver).

- **Lỗ hổng thoát Sandbox trong Google Chrome - CVE-2026-76023** - Lỗ hổng kiểm soát tài nguyên không phù hợp nằm trong thành phần Linux Toolkit Theming của trình duyệt Google Chrome.

- **Lỗ hổng Race Condition trong Linux Kernel GPIO PCA953x Driver - CVE-2026-74733** - Lỗ hổng xảy ra do tranh chấp khóa tài nguyên không phù hợp trong trình điều khiển PCA953x thuộc nhân Linux.

- **Lỗi hỏng OS Command Injection trong Dell Virtual Storage Integrator – CVE-2026-67261** - Lỗi hỏng chèn lệnh hệ điều hành phát sinh do thành phần IAPI của Dell Virtual Storage Integrator (VSI) cho VMware vSphere Client xử lý các lệnh hệ điều hành không an toàn.

- **Lỗi hỏng tiết lộ thông tin nhạy cảm trong Dell Virtual Storage Integrator - CVE-2026-54489** - Lỗi hỏng tiết lộ thông tin nhạy cảm xảy ra do cơ chế bảo vệ dữ liệu trong Dell Virtual Storage Integrator chưa đầy đủ.

- **Lỗi hỏng vắng mặt xác thực trong VMware vCenter Server - CVE-2026-59309** - Lỗi hỏng vượt qua cơ chế xác thực phát sinh do thuật toán xác thực của dịch vụ thư mục VMware Directory Service (vmdir) trong VMware vCenter Server được triển khai không chính xác (CWE-303).

- **Lỗi hỏng sử dụng thông tin xác thực cứng trong các dòng Router TP-Link - CVE-2026-12001** - Lỗi hỏng tồn tại do dữ liệu xác thực được lưu trực tiếp trong tệp mật khẩu thuộc mã nguồn firmware.

- **Lỗi hỏng thực thi mã từ xa trong các dòng Switch Cisco Nexus 9000 - CVE-2026-20212** - Lỗi hỏng thực thi mã từ xa phát sinh do một dịch vụ trên thiết bị liên kết với địa chỉ IP không bị giới hạn qua cổng TCP 43210 và 43211.

- **Lỗi hỏng thực thi mã từ xa trong Microsoft Outlook - CVE-2026-70329** - Microsoft Outlook Remote Code Execution Vulnerability Lỗi hỏng phát sinh do lỗi tràn số nguyên trong quá trình xử lý tệp tin Office được chế tạo đặc biệt.

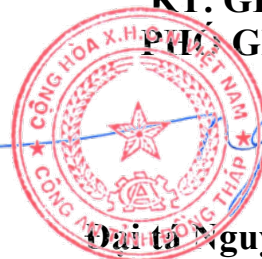
- **Lỗi hỏng tải tệp tùy ý không cần xác thực trong Elementor Pro - CVE-2026-32475** - Lỗi hỏng phát sinh do sự bất đồng bộ giữa vòng lặp kiểm tra và xử lý tải tệp tại tính năng Form File Upload.

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 lỗi hỏng và các biện pháp phòng ngừa).

Nơi nhận:

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

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC



Đại tá Nguyễn Minh Tân

PHỤ LỤC

(Kèm theo Công văn số: 8229/CAT-ANM, ngày 16 / 09/2026 của Công an tỉnh)

1. Lỗ hổng thực thi mã từ xa trong Microsoft SharePoint Server - CVE-2026-50522 - Lỗ hổng phát sinh từ cơ chế xử lý dữ liệu không an toàn trong Microsoft SharePoint Server.

a) Mô tả

- Điểm CVSS: 9.8;
- Mức độ: Critical;
- Lỗ hổng phát sinh từ cơ chế xử lý dữ liệu không an toàn trong Microsoft SharePoint Server. Bằng cách gửi một yêu cầu được thiết kế chứa dữ liệu không tin cậy đến hệ thống, đối tượng có thể kích hoạt lỗi và thực thi mã tùy ý trực tiếp trên máy chủ SharePoint.

- Lỗ hổng tiềm ẩn nguy cơ cao đối với các cơ quan, tổ chức nhà nước đang triển khai sử dụng hệ thống SharePoint On-Premises để quản lý văn bản, lưu trữ tài liệu nội bộ hoặc làm cổng trao đổi thông tin hạ tầng.

Các phiên bản bị ảnh hưởng bao gồm:

Microsoft SharePoint Enterprise Server 2016 (trước bản cập nhật 16.0.5561.1001).

Microsoft SharePoint Server 2019 (trước bản cập nhật 16.0.10417.20175).

Microsoft SharePoint Server Subscription Edition (trước bản cập nhật 16.0.19725.20434).

b) Kiến nghị

- Các tổ chức, đơn vị đang triển khai Microsoft SharePoint Server On-Premises cần chủ động rà soát hệ thống và nhanh chóng áp dụng bản cập nhật bảo mật chính thức mới nhất từ Microsoft cho các phiên bản SharePoint đang sử dụng.

- Thắt chặt chính sách kiểm soát truy cập đối với cổng dịch vụ SharePoint, hạn chế mở giao diện quản trị hoặc cổng nội bộ trực tiếp ra môi trường Internet khi chưa qua các lớp bảo vệ như WAF, Firewall hoặc kết nối VPN/Out-of-Band.

- Tiến hành rà soát nhật ký hệ thống trên các máy chủ SharePoint để kịp thời phát hiện các dấu hiệu bất thường hoặc các yêu cầu HTTP có dấu hiệu can thiệp dữ liệu trái phép.

2. Lỗi hỏng thực thi mã từ xa trong Windows IKE Extension - CVE-2026-33824 - Lỗi hỏng phát sinh từ lỗi giải phóng bộ nhớ hai lần trong thành phần Windows IKE Extension.

a) Mô tả

- Điểm CVSS: 9.8;
- Mức độ: Critical;
- Lỗi hỏng phát sinh từ lỗi giải phóng bộ nhớ hai lần trong Windows IKE Extension. Đối tượng không cần xác thực hay được quyền truy cập vào hệ thống, mà chỉ cần gửi các gói tin được tạo đặc biệt đến thiết bị Windows đang bật giao thức IKEv2 là có thể kích hoạt lỗi hỏng, dẫn đến khả năng thực thi mã từ xa với đặc quyền cao.
- Lỗi hỏng ảnh hưởng trực tiếp đến các hệ thống Windows Server và Windows client có kích hoạt hoặc sử dụng dịch vụ VPN/IPsec dựa trên giao thức IKEv2.

b) Kiến nghị

- Các đơn vị cần nhanh chóng kiểm tra và cập nhật bản vá bảo mật mới nhất từ Microsoft cho tất cả các máy.
- Rà soát các thiết bị, máy chủ đang sử dụng giao thức IKEv2 (cổng UDP 500 và UDP 4500), nếu không thực sự cần thiết, nên tạm thời hạn chế hoặc ngắt kết nối dịch vụ IKEv2 từ mạng công cộng Internet cho đến khi bản vá được áp dụng hoàn tất.
- Triển khai giám sát, phát hiện bất thường trên hệ thống tường lửa và giải pháp IDS/IPS để kịp thời ngăn chặn các gói tin IKEv2 bất thường nhằm vào hạ tầng mạng.

3. Lỗi hỏng leo thang đặc quyền trong Windows Ancillary Function Driver for WinSock - CVE-2026-68820 - Lỗi hỏng phát sinh từ lỗi giải phóng bộ nhớ nhưng vẫn tiếp tục sử dụng trong trình điều khiển AFD.sys (Windows Ancillary Function Driver for WinSock).

a) Mô tả

- Điểm CVSS: 7.8;
- Mức độ: High;
- Lỗi hỏng phát sinh từ lỗi giải phóng bộ nhớ nhưng vẫn tiếp tục sử dụng trong trình điều khiển AFD.sys (Windows Ancillary Function Driver for WinSock). Đối tượng đã xác thực cục bộ chạy một ứng dụng được kích hoạt tranh chấp, từ đó nâng cao đặc quyền và giành quyền kiểm soát tối cao SYSTEM trên hệ thống.
- Lỗi hỏng ảnh hưởng trực tiếp đến các hệ điều hành Windows Server và Windows client có thành phần AFD.sys hỗ trợ kết nối mạng WinSock.

b) Kiến nghị

- Các đơn vị cần sử dụng bản cập nhật bảo mật mới nhất từ Microsoft cho toàn bộ các máy.
- Giới hạn và kiểm soát chặt chẽ quyền chạy tệp thi hành (.exe, .bat, .ps1) của người dùng, triển khai chính sách hạn chế ứng dụng (AppLocker/WDAC) để ngăn chặn việc thực thi các tệp tin độc.
- Tăng cường giám sát nhật ký hệ thống và triển khai giải pháp EDR để phát hiện sớm các hành vi bất thường liên quan đến việc khởi tạo tiến trình mới dưới quyền SYSTEM từ tài khoản người dùng hạn chế.

4. Lỗ hổng leo thang đặc quyền trong Windows User Profile Service - CVE-2026-62832 - Lỗ hổng phát sinh do cơ chế xử lý liên kết (symlink/junction) trước khi truy cập tệp không phù hợp trong dịch vụ Windows User Profile Service.

a) Mô tả

- Điểm CVSS: 7.8;
- Mức độ: High;
- Lỗ hổng phát sinh do cơ chế xử lý liên kết (symlink/junction) trước khi truy cập tệp không phù hợp trong dịch vụ Windows User Profile Service. Đối tượng đã xác thực và sở hữu thông tin đăng nhập của một tài khoản cục bộ khác có thể chạy một ứng dụng được tạo đặc biệt để tải tệp cấu hình registry (registry hive) của người dùng khác. Khai thác thành công cho phép đối tượng truy cập, sửa đổi dữ liệu riêng tư của người dùng đó và nâng đặc quyền lên quyền quản trị viên (Administrator).
- Lỗ hổng ảnh hưởng đến dịch vụ quản lý hồ sơ người dùng trên các hệ điều hành Windows Server và Windows client.

b) Kiến nghị

- Các cơ quan, tổ chức cần nhanh chóng kiểm tra và áp dụng bản cập nhật bảo mật chính thức mới nhất từ Microsoft cho tất cả các máy trạm và máy chủ Windows trong hệ thống.
- Rà soát, quản lý chặt chẽ danh sách tài khoản người dùng cục bộ; áp dụng nguyên tắc đặc quyền tối thiểu, vô hiệu hóa các tài khoản không sử dụng và hạn chế quyền tạo chia sẻ tài khoản dùng chung trên cùng một máy tính.
- Triển khai các giải pháp giám sát EDR và chính sách kiểm soát ứng dụng (AppLocker/WDAC) nhằm phát hiện, ngăn chặn việc thực thi các ứng dụng bất thường có hành vi can thiệp vào registry hive hoặc liên kết tệp hệ thống của người dùng khác.

5. Lỗ hổng giả mạo dữ liệu trong Windows Container Isolation FS Filter Driver - CVE-2026-72971 - Lỗ hổng liên quan đến cơ chế xử lý liên kết tệp trong trình điều khiển unionfs.sys (Windows Container Isolation FS Filter Driver).

a) Mô tả

- Điểm CVSS: 7.8;
- Mức độ: High;
- Lỗ hổng liên quan đến cơ chế xử lý liên kết tệp trong trình điều khiển unionfs.sys (Windows Container Isolation FS Filter Driver). Đối tượng đã được xác thực cục bộ có thể lợi dụng việc này để thực hiện hành vi giả mạo hoặc thay đổi dữ liệu trái phép trên hệ thống, làm phá vỡ tính toàn vẹn của các tệp tin và hành vi cách ly của môi trường container.

- Lỗ hổng được phát hiện bởi các nhà nghiên cứu bảo mật yhw và txz.

b) Kiến nghị

- Ưu tiên áp dụng bản vá bảo mật của Microsoft đối với các máy chủ vận hành hạ tầng container hoặc chạy khối lượng công việc dạng containerized.
- Kiểm tra tính toàn vẹn của hệ thống tệp và giám sát chặt chẽ các hành vi chỉnh sửa cấu hình dữ liệu trái phép trong các phân vùng isolated container.

6. Lỗ hổng thoát Sandbox trong Google Chrome - CVE-2026-76023 - Lỗ hổng kiểm soát tài nguyên không phù hợp nằm trong thành phần Linux Toolkit Theming của trình duyệt Google Chrome.

a) Mô tả

- Điểm CVSS: 8.8;
- Mức độ: High;
- Lỗ hổng kiểm soát tài nguyên không phù hợp nằm trong thành phần Linux Toolkit Theming của trình duyệt Google Chrome. Đối tượng từ xa sau khi đã chiếm quyền kiểm soát tiến trình xử lý giao diện có thể dụ người dùng truy cập một trang HTML được thiết kế đặc biệt để thực thi mã tùy ý bên ngoài môi trường cách ly (sandbox escape).

- Lỗ hổng ảnh hưởng đến trình duyệt Google Chrome trên hệ điều hành Linux trước phiên bản 151.0.7922.173.

b) Kiến nghị

- Khẩn trương nâng cấp trình duyệt Google Chrome trên các máy trạm Linux lên phiên bản 151.0.7922.173 hoặc mới hơn.

- Khuyến cáo người dùng hạn chế truy cập vào các liên kết lạ hoặc tệp HTML không rõ nguồn gốc để giảm thiểu nguy cơ bị thực thi mã độc thoát sandbox.

7. Lỗi hỏng Race Condition trong Linux Kernel GPIO PCA953x Driver - CVE-2026-74733 - Lỗi hỏng xảy ra do tranh chấp khóa tài nguyên không phù hợp trong trình điều khiển PCA953x thuộc Linux.

a) Mô tả

- Điểm CVSS: 4.7;
- Mức độ: Medium;
- Lỗi hỏng xảy ra do tranh chấp khóa tài nguyên không phù hợp trong trình điều khiển PCA953x thuộc nhân Linux. Hàm `pca953x_irq_bus_sync_unlock()` không duy trì đúng khóa `i2c_lock` khi thao tác với `regmap`, dẫn đến việc nhiều luồng (threads) truy cập đồng thời gây ra lỗi đọc ghi sai thanh ghi. Khai thác thành công có thể làm sai lệch dữ liệu thanh ghi và ảnh hưởng trực tiếp đến hoạt động của các thiết bị giao tiếp GPIO.

- Lỗi hỏng ảnh hưởng đến tất cả các nhân Linux Kernel có bật và sử dụng trình điều khiển PCA953x.

b) Kiến nghị

- Tiến hành cập nhật Linux Kernel lên phiên bản mới nhất đã bao gồm bản vá sửa lỗi đồng bộ cho driver PCA953x.
- Đánh giá và kiểm soát các luồng truy cập vào thiết bị phần cứng GPIO/I2C trên hệ thống để tránh nguy cơ gián đoạn hoặc vận hành sai lệch thiết bị.

8. Lỗi hỏng OS Command Injection trong Dell Virtual Storage Integrator - CVE-2026-67261 - Lỗi hỏng chèn lệnh hệ điều hành phát sinh do thành phần IAPI của Dell Virtual Storage Integrator (VSI) cho VMware vSphere Client xử lý các lệnh hệ điều hành không an toàn.

a) Mô tả

- Điểm CVSS: 9.8;
- Mức độ: Critical;
- Lỗi hỏng chèn lệnh hệ điều hành phát sinh do thành phần IAPI của Dell Virtual Storage Integrator (VSI) cho VMware vSphere Client xử lý các lệnh hệ điều hành không an toàn. Đối tượng từ xa không cần xác thực có thể gửi các yêu cầu đặc chế để thực thi các lệnh hệ điều hành tùy ý với đặc quyền tối cao (root), từ đó dẫn đến nguy cơ kiểm soát hoàn toàn hệ thống.

- Lỗ hổng ảnh hưởng đến Dell Virtual Storage Integrator for VMware vSphere Client trước phiên bản 10.11.1.0.

b) Kiến nghị

- Khẩn trương nâng cấp Dell Virtual Storage Integrator lên phiên bản 10.11.1.0 hoặc mới hơn theo khuyến cáo chính thức từ Dell để khắc phục triệt để lỗ hổng.

- Thắt chặt chính sách tường lửa, hạn chế diện tiếp xúc của giao diện quản trị vSphere Client và các thành phần VSI từ môi trường mạng không tin cậy.

9. Lỗ hổng tiết lộ thông tin nhạy cảm trong Dell Virtual Storage Integrator

- CVE-2026-54489 - Lỗ hổng tiết lộ thông tin nhạy cảm xảy ra do cơ chế bảo vệ dữ liệu trong Dell Virtual Storage Integrator chưa đầy đủ.

a) Mô tả

- Điểm CVSS: 9.1;

- Mức độ: Critical;

- Lỗ hổng tiết lộ thông tin nhạy cảm phát sinh do cơ chế bảo vệ dữ liệu trong Dell Virtual Storage Integrator (VSI) for VMware vSphere Client chưa đầy đủ. Đối tượng từ xa không cần xác thực có thể khai thác điểm yếu này để thu thập thông tin xác thực của các phiên làm việc đang hoạt động, từ đó thực hiện chiếm quyền điều khiển phiên.

- Khai thác thành công cho phép đối tượng giả mạo hoàn toàn người dùng đã được xác thực trên hệ thống, bao gồm cả các tài khoản có đặc quyền quản trị viên.

- Lỗ hổng ảnh hưởng đến các phiên bản Dell Virtual Storage Integrator trước 10.11.1.0.

b) Kiến nghị

- Cập nhật Dell Virtual Storage Integrator lên phiên bản 10.11.1.0 hoặc mới hơn ngay lập tức.

- Thực hiện đăng xuất và hủy bỏ toàn bộ các phiên làm việc hiện có, đồng thời đặt lại thông tin xác thực tokens sau khi nâng cấp để triệt tiêu nguy cơ đối tượng tiếp tục lợi dụng các phiên đã thu thập từ trước.

- Thắt chặt phân vùng mạng, hạn chế quyền truy cập vào giao diện quản trị vSphere Client và các thành phần VSI từ các vùng mạng không tin cậy.

10. Lỗ hổng vắng mặt xác thực trong VMware vCenter Server - CVE-2026-

59309 - Lỗ hổng vượt qua cơ chế xác thực phát sinh do thuật toán xác thực của dịch

vụ thư mục VMware Directory Service (vmdir) trong VMware vCenter Server được triển khai không chính xác (CWE-303).

a) Mô tả

- Điểm CVSS: 9.8;
- Mức độ: Critical;
- Lỗ hổng vượt qua cơ chế xác thực phát sinh do thuật toán xác thực của thư mục VMware Directory Service (vmdir) trong VMware vCenter Server được triển khai không chính xác (CWE-303). Đối tượng có kết nối mạng tới máy chủ vCenter có thể lợi dụng điểm yếu này để vượt qua lớp bảo vệ mà không cần tài khoản, dẫn đến mất hoàn toàn tính bảo mật và chiếm quyền kiểm soát trái phép hệ thống quản trị vCenter.

- Lỗ hổng ảnh hưởng đến các phiên bản VMware vCenter Server có triển khai VMware Directory Service.

b) Kiến nghị

- Áp dụng ngay bản cập nhật bảo mật mới nhất từ VMware cho các máy chủ vCenter Server bị ảnh hưởng.
- Cách ly giao diện quản trị vCenter Server, chỉ cho phép truy cập từ các phân vùng mạng nội bộ (Internal/Management Network) hoặc qua VPN/Bastion Host có kiểm soát Access Control List (ACL) nghiêm ngặt.

11. Lỗ hổng sử dụng thông tin xác thực cứng trong các dòng Router TP-Link - CVE-2026-12001 - Lỗ hổng tồn tại do dữ liệu xác thực được lưu trực tiếp trong tệp mật khẩu thuộc mã nguồn firmware.

a) Mô tả

- Điểm CVSS: 5.2;
- Mức độ: Medium;
- Lỗ hổng sử dụng thông tin xác thực cứng (CWE-798) phát sinh trong mã nguồn firmware của nhiều dòng router TP-Link. Đối tượng có thể thu thập và trích xuất thông tin mật khẩu thông qua việc phân tích và giải mã firmware của thiết bị.
- Khai thác thành công cho phép đối tượng truy cập trái phép vào các chức năng có đặc quyền quản trị trên thiết bị bị ảnh hưởng.
- Lỗ hổng ảnh hưởng đến các dòng thiết bị TP-Link chưa cập nhật phiên bản vá lỗi, bao gồm:

TL-WR845N v4 (trước bản build UN_V4_250401), TL-WR850N v3 (trước bản build IN_V3.48_3.16.0 Build 260422_2048), TL-WR902AC v4 (trước các bản build US_V4_0.9.1 / EU_V4_0.9.3), Archer C20 v6 (trước bản build US_V6_250630), và Archer MR200 v5 (trước bản build EU_V5.20_1.3.0).

b) Kiến nghị

- Cập nhật firmware lên phiên bản mới nhất đã được khắc phục lỗi cho từng router tương ứng.

- Thay thế thiết bị bằng các mẫu thiết bị mới nếu dòng router đang sử dụng không còn được nhà sản xuất phát hành bản cập nhật vá lỗi.

- Áp dụng các quy trình quản lý thông tin xác thực an toàn và kiểm soát chặt chẽ quyền truy cập cũng như giao diện quản trị của thiết bị.

12. Lỗ hổng thực thi mã từ xa trong các dòng Switch Cisco Nexus 9000 - CVE-2026-20212 - Lỗ hổng thực thi mã từ xa phát sinh do một dịch vụ trên thiết bị liên kết với địa chỉ IP không bị giới hạn qua cổng TCP 43210 và 43211.

a) Mô tả

- Điểm CVSS: 9.8;

- Mức độ: Critical;

- Lỗ hổng thực thi mã từ xa (CVE-2026-20212) xuất phát từ việc một dịch vụ trên thiết bị liên kết với địa chỉ IP không bị giới hạn, khiến hai cổng TCP 43210 và 43211 có thể bị truy cập từ mạng thông qua VRF mặc định. Đối tượng từ xa không cần xác thực có thể gửi các dữ liệu được chế tạo đặc biệt tới dịch vụ qua các cổng này.

- Khai thác thành công cho phép đối tượng thực thi mã tùy ý với quyền root, chiếm quyền kiểm soát thiết bị ở mức cao, đồng thời có thể làm dừng tiến trình S1HAL và khiến thiết bị bị tải lại (gây từ chối dịch vụ).

- Lỗ hổng ảnh hưởng đến 10 mẫu switch Cisco Nexus 9000 sử dụng chip Silicon One (bao gồm: N9324C-SE1U, N9348Y2C6D-SE1U, N9364E-SG2-O, N9364E-SG2-Q, N9396T12C-SE1, N9348Y12C-SE1, N9396Y12C-SE1, N9336C-SE1, N9K-C9804 và N9K-C9808), thuộc phạm vi 45 phiên bản NX-OS từ 10.3(1) đến 10.6(3s). Các dòng Nexus 9000 khác, Nexus 9000 chạy chế độ ACI, Nexus 3000 và Nexus 7000 không bị ảnh hưởng.

b) Kiến nghị

- Quản trị viên sử dụng thiết bị thuộc phạm vi ảnh hưởng cần kiểm tra ngay phiên bản phần mềm (sử dụng công cụ Software Checker của Cisco) và ưu tiên nâng cấp lên phiên bản NX-OS mới nhất theo hướng dẫn của Cisco.

- Trong thời gian chưa thể cập nhật, áp dụng ngay biện pháp giảm thiểu tạm thời bằng cách cấu hình iACL để ngăn chặn hạn chế kết nối từ mạng tới cổng TCP 43210 và 43211, hoặc sử dụng giải pháp Live Protect Shield tạm thời đối với các phiên bản NX-OS được hỗ trợ. Đối với thiết bị chạy IOS XR liên quan, kiểm tra bảng SMU của Cisco để xác định bản cập nhật tương ứng.

- Ưu tiên xử lý khẩn cấp do đây là thiết bị nằm ở lớp hạ tầng mạng quan trọng có quyền kiểm soát lưu lượng lớn, dù tại thời điểm công bố chưa ghi nhận bằng chứng khai thác trong thực tế.

13. Lỗ hổng thực thi mã từ xa trong Microsoft Outlook - CVE-2026-70329 - Microsoft Outlook Remote Code Execution Vulnerability Lỗ hổng phát sinh do lỗi tràn số nguyên trong quá trình xử lý tệp tin Office được chế tạo đặc biệt.

a) Mô tả

- Điểm CVSS: 8.8;
- Mức độ: High;
- Lỗ hổng thực thi mã từ xa phát sinh do lỗi xử lý bộ nhớ vượt quá giới hạn dữ liệu số nguyên (CWE-190) trong Microsoft Outlook. Kẻ tấn công có thể lợi dụng kịch bản lừa đảo (Phishing) đính kèm tệp tin tài liệu Office độc hại và dụ dỗ người dùng mở tệp.
- Khai thác thành công cho phép kẻ tấn công thực thi mã tùy ý (RCE) trên hệ thống nạn nhân theo quyền hạn của người dùng hiện tại, dẫn đến nguy cơ chiếm quyền kiểm soát máy trạm, cài đặt mã độc hoặc sử dụng máy xâm nhập sâu vào mạng nội bộ.
- Lỗ hổng ảnh hưởng đến các phiên bản: Microsoft 365 Apps for Enterprise, Office 2019, Office LTSC 2021, Office LTSC 2024 và Microsoft Outlook 2016.

b) Kiến nghị

- Cập nhật ngay bản vá mới nhất của Microsoft cho các ứng dụng Office / Outlook trên toàn bộ hệ thống.
- Tăng cường hệ thống lọc email lừa đảo và ngăn chặn các tệp tin đính kèm nghi vấn từ nguồn không tin cậy.
- Nâng cao nhận thức an toàn thông tin cho người dùng, khuyến cáo không mở các tệp tin tài liệu lạ hoặc đính kèm email không xác định.

14. Lỗ hổng tải tệp tùy ý không cần xác thực trong Elementor Pro - CVE-2026-32475 - Lỗ hổng phát sinh do sự bất đồng bộ giữa vòng lặp kiểm tra và xử lý tải tệp tại tính năng Form File Upload.

a) Mô tả

- Điểm CVSS: 9.8;

- Mức độ: Critical;

- Lỗ hổng Unauthenticated Arbitrary File Upload xuất hiện trong plugin Elementor Pro trên WordPress. Do lỗi xử lý dữ liệu tải tệp rỗng, kẻ tấn công không cần đăng nhập có thể gửi yêu cầu multipart đặc biệt để bỏ qua cơ chế kiểm tra định dạng tệp và tải trực tiếp tệp PHP độc hại lên thư mục wp-content/uploads/elementor/forms/.

- Khai thác thành công cho phép kẻ tấn công thực thi mã từ xa (RCE) qua webshell, chiếm quyền quản trị trang web WordPress, tạo tài khoản ẩn, chèn mã độc chuyển hướng hoặc đánh cắp toàn bộ cơ sở dữ liệu. Lỗ hổng hiện đang bị khai thác hàng loạt trên môi trường Internet đối với các trang web có sử dụng Form widget chứa trường Upload.

- Lỗ hổng ảnh hưởng đến plugin Elementor Pro từ phiên bản 4.2.1 trở xuống (Elementor Pro <= 4.2.1).

b) Kiến nghị

- Nâng cấp plugin Elementor Pro lên phiên bản 4.2.2 hoặc mới hơn để khắc phục triệt để lỗ hổng.

- Rà soát hệ thống tệp tin trong thư mục wp-content/uploads/elementor/forms/ để phát hiện và gỡ bỏ các tệp tin .php lạ hoặc webshell.

- Cấu hình máy chủ web (Nginx/Apache) vô hiệu hóa quyền thực thi tệp PHP trực tiếp trong thư mục uploads/ và triển khai Tường lửa ứng dụng Web (WAF) để ngăn chặn hành vi tải tệp bất thường.