BỘ CÔNG AN
CÔNG AN TỈNH QUẢNG NGÃI

Số: 1048/CAT-ANM
V/v cảnh báo lỗ hổng bảo mật nghiêm trọng tháng 01/2026

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

Quảng Ngãi, ngày 26 tháng 02 năm 2026

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 01/2026, qua công tác bảo đảm an toàn thông tin, lực lượng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao Công an tỉnh đã thực hiện phân tích và tổng hợp đối với **18** 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, 12 lỗ hổng bảo mật nghiêm trọng, 01 lỗ hổng bảo mật mức trung bình, cụ thể:

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

1.1. CVE-2026-20944 – Lỗ hổng thực thi mã (RCE) không cần tương tác trong Microsoft Office Word

- Đánh giá mức độ nguy hiểm: Cao (điểm CVSS: 8.4/10).

- Mô tả kỹ thuật:

+ Lỗ hổng phát sinh từ cơ chế xử lý tài liệu Word trong các trường hợp không yêu cầu tương tác người dùng. Khi Word tự động phân tích cấu trúc tài liệu hoặc đối tượng nhúng được tạo lập bất thường trong tệp, lỗi quản lý bộ nhớ có thể xảy ra và dẫn đến thực thi mã với quyền người dùng. Do không cần thao tác mở tệp thủ công, lỗ hổng này đặc biệt nguy hiểm trong các hệ thống xử lý tài liệu tự động.

+ Tình huống khai thác: Tin tặc gửi tệp Word độc hại được thiết kế đặc biệt đến hệ thống tiếp nhận, xử lý văn bản tự động của cơ quan. Khi hệ thống tự quét và xử lý tệp Word, mã độc được thực thi, cài backdoor và mở kết nối ra ngoài, cho

phép tin tặc tấn công truy cập vào mạng nội bộ và tiếp tục dò quét các máy khác.

- Phiên bản ảnh hưởng: Các phiên bản Word thuộc Office 2016, 2019, 2021 và Microsoft 365 Apps.

- Khuyến nghị: Cập nhật, áp dụng bản vá lỗi do Microsoft phát hành https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-20944

1.2. CVE-2026-20947 – Lỗ hổng thực thi mã (RCE) và leo thang đặc quyền trong Microsoft Office SharePoint

- Đánh giá mức độ nguy hiểm: Cao (điểm CVSS: 8.8/10).

- Mô tả kỹ thuật:

+ Lỗ hổng phát sinh từ cơ chế xử lý yêu cầu mạng trong SharePoint khi người dùng đã xác thực với quyền thấp. Kẻ tấn công có thể gửi các yêu cầu được thiết kế đặc biệt đến máy chủ SharePoint, lợi dụng lỗi kiểm tra dữ liệu đầu vào để thực thi mã hoặc chiếm quyền điều khiển dịch vụ. Lỗ hổng này nguy hiểm do có thể bị khai thác từ xa qua mạng và ảnh hưởng trực tiếp đến hệ thống máy chủ.

+ Tình huống khai thác: Tin tặc sử dụng tài khoản người dùng quyền tập đã bị lộ để gửi chuỗi yêu cầu HTTP đặc biệt tới máy chủ sharepoint, sau khi khai thác thành công, tin tặc có thể chiếm quyền điều khiển máy chủ, truy xuất dữ liệu nội bộ và cài công cụ duy trì truy cập lâu dài *(persistence)*.

- Phiên bản ảnh hưởng: Tất cả các phiên bản Sharepoint Server chưa được cài đặt bản vá của nhà sản xuất.

- Khuyến nghị: Khẩn trương cập nhật, áp dụng bản vá do Microsoft phát hành: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-20947

1.3. CVE-2026-20952 - Lỗ hổng thực thi mã qua đối tượng nhúng trong Microsoft Office

- Đánh giá mức độ nguy hiểm: Cao (điểm CVSS: 8.4/10).

- Mô tả kỹ thuật:

+ Lỗ hổng phát sinh trong thành phần xử lý đối tượng và nội dung nhúng chung của bộ Office *(nơi chịu trách nhiệm phân tích và hiển thị các đối tượng OLE/ActiveX trong tài liệu)*. Khi Office xử lý các đối tượng nhúng được tạo lập với cấu trúc bất thường hoặc dữ liệu bị thao túng, cơ chế quản lý bộ nhớ không kiểm tra tính hợp lệ của dữ liệu đầu vào, dẫn đến thực thi mã tùy ý.

+ Tình huống khai thác: Một tệp tài liệu Office được tin tặc nhúng mã độc khai thác lỗ hổng và tán phát trên hệ thống trao đổi văn bản của cơ quan hoặc gửi có chủ đích qua email đến người dùng. Khi hệ thống xử lý tài liệu tự động hoặc người dùng mở preview tệp, lỗ hổng được kích hoạt và mã độc được thực thi, cài đặt cửa hậu, thiết lập kết nối máy chủ C2 của tin tặc.

- Phiên bản ảnh hưởng: Phiên bản Office 2016 trở lên và Microsoft 365 Apps.

- Khuyến nghị: Khẩn trương cập nhật, áp dụng bản vá do Microsoft phát hành: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-20952

1.4. CVE-2026-20953 - Lỗ hổng thực thi mã do xử lý dữ liệu đầu vào không an toàn trong Microsoft Office

- Đánh giá mức độ nguy hiểm: Cao (điểm CVSS: 8.4/10).

- Mô tả kỹ thuật:

+ Lỗ hổng phát sinh trong từ việc Office xử lý sai kiểu dữ liệu của một số đối tượng trong tài liệu. Khi gặp dữ liệu giả mạo hoặc khai báo sai định dạng, chương trình vẫn cố gắng xử lý mà không kiểm tra đầy đủ, dẫn đến truy cập nhầm vùng nhớ và tạo điều kiện cho mã độc thực thi.

+ Tình huống khai thác: Tin tặc nhắm đến một cá nhân có quyền truy cập cao trong hệ thống và gửi tài liệu giả mạo nội dung công việc được nhúng mã độc. Khi nạn nhân mở tài liệu, lỗi xử lý kiểu dữ liệu trong Office bị khai thác cho phép tin tặc thực thi mã với quyền người dùng, từ đó cài công cụ đánh cắp thông tin xác thực, chiếm phiên làm việc và truy cập vào các hệ thống quan trọng, leo thang đặc quyền và đánh cắp dữ liệu quan trọng trong hệ thống.

- Phiên bản ảnh hưởng: Phiên bản Office 2016, 2019, 2021 và Microsoft 365 Apps.

- Khuyến nghị: Không tải về, mở các tệp tài liệu lạ, không rõ nguồn gốc. Khẩn trương cập nhật, áp dụng bản vá do Microsoft phát hành: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-20953

1.5. CVE-2026-24307 – Lỗ hổng rò rỉ thông tin và vượt quyền truy cập (Information Disclosure/Authorization bypass) trong Microsoft 365 Copilot

- Đánh giá mức độ nguy hiểm: Rất cao (điểm CVSS: 9.3/10).

- Mô tả kỹ thuật:

+ Lỗ hổng phát sinh từ cơ chế xử lý yêu cầu và kiểm soát phân quyền trong Microsoft 365 Copilot khi hệ thống tổng hợp dữ liệu từ nhiều nguồn khác nhau. Trong một số trường hợp, Copilot không kiểm tra đầy đủ phạm vi quyền truy cập trước khi trả lời truy vấn của người dùng, khiến thông tin nhạy cảm có thể bị tiết lộ vượt ngoài quyền cho phép.

+ Tình huống khai thác: Tin tặc trước tiên xâm nhập vào môi trường hệ thống với quyền hạn thấp (tài khoản guest, các tài khoản bị lộ mà tin tặc khai thác được), tải lên môi trường chung của hệ thống *(Sharepoint, Onedrive, Teams dùng chung)* tài liệu được tạo lập chứa nội dung được thiết kế đặc biệt *(có thể ảnh hưởng đến cách Copilot thu thập và tổng hợp dữ liệu)*, sau đó trực tiếp truy vấn Copilot bằng các câu hỏi có chủ đích yêu cầu cung cấp dữ liệu nhạy cảm. Do lỗi kiểm soát phân quyền, Copilot trong quá trình tổng hợp câu trả lời có thể truy xuất thông tin từ các nguồn mà tài khoản đó lẽ ra không được phép xem, dẫn đến rò rỉ dữ liệu.

- Phiên bản ảnh hưởng: Các hệ thống, môi trường có triển khai Microsoft 365 Copilot.

- Khuyến nghị: Khẩn trương cập nhật, áp dụng bản vá do Microsoft phát hành: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-24307.

1.6. CVE-2026-21264 – Lỗ hổng chiếm quyền tài khoản trên Microsoft Account.

- Đánh giá mức độ nguy hiểm: Rất cao (điểm CVSS: 9.3/10).

- Mô tả kỹ thuật:

+ Lỗ hổng phát sinh từ sai sót trong cơ chế xác thực và quản lý phiên đăng nhập của hệ thống Microsoft Account. Trong một số tình huống xử lý đăng nhập hoặc duy trì phiên làm việc, hệ thống không kiểm tra đầy đủ tính hợp lệ của yêu cầu và trạng thái phiên, tạo ra kẽ hở để kẻ tấn công chiếm quyền truy cập tài khoản. Nói một cách đơn giản, cơ chế bảo vệ phiên đăng nhập chưa đủ chặt chẽ, khiến tin tặc có thể lợi dụng để giả mạo hoặc chiếm quyền phiên của người dùng hợp pháp.

+ Tình huống khai thác: Tin tặc có thể lợi dụng lỗ hổng để thực hiện một cuộc tấn công chiếm quyền phiên đăng nhập *(session hijacking)* vào hệ thống Microsoft Account, cụ thể đối tượng chuẩn bị một trang web hoặc dịch vụ trung gian được xây dựng nhằm khai thác sai sót trong cơ chế xác thực. Khi người dùng truy cập và đăng nhập Microsoft Account qua môi trường này, session token hợp lệ có thể bị rò rỉ hoặc bị chiếm đoạt. Sau đó, tin tặc sử dụng token này để giả mạo người dùng và truy cập trái phép vào tài khoản mà không cần mật khẩu. Khi đã chiếm được phiên đăng nhập, tin tặc có thể truy cập email, dữ liệu đám mây và các dịch vụ liên kết với Microsoft Account, từ đó mở rộng xâm nhập vào hệ thống thông tin.

- Phiên bản ảnh hưởng: Người dùng Microsoft Account trên phạm vi rộng.

- Khuyến nghị: Khẩn trương cập nhật, áp dụng bản vá do Microsoft phát hành: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-24307

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

CVE-2026-24061 – Lỗ hổng bảo mật nghiêm trọng Authemtication Bypass

- Đánh giá mức độ nguy hiểm: Rất cao (điểm CVSS: 9.8/10).

- Mô tả kỹ thuật:

+ Lỗ hổng cho phép vượt qua xác thực từ xa (Remote Authentication Bypass) trong dịch vụ telnetd của bộ công cụ GNU Inetutils. Cụ thể, kẻ tấn công có thể khai thác thông qua biến môi trường USER. Bằng cách gửi một giá trị đặc biệt như -f root cho biến môi trường này khi kết nối, kẻ tấn công có thể đánh lừa hệ thống để đăng nhập trực tiếp với quyền root mà không cần cung cấp mật khẩu. Lỗi này phát sinh từ việc xử lý tham số đầu vào không an toàn trong mã nguồn của telnetd. Cho phép kẻ tấn công đăng nhập vào hệ thống mà không cần mật khẩu, thậm chí chiếm quyền quản trị của máy chủ

- Phiên bản ảnh hưởng: Tất cả các phiên bản GNU Inetutils cho đến 2.7. Trên Ubuntu, các phiên bản bị ảnh hưởng bao gồm: Ubuntu 25.10 (Questing); Ubuntu 24.04 LTS (Noble); Ubuntu 22.04 LTS (Jammy); Ubuntu 20.04 LTS (Focal) và các bản cũ hơn (đang được đánh giá).

- Khuyến nghị:

+ Cập nhật bản vá: Nâng cấp gói inetutils-telnetd lên phiên bản mới nhất đã được sửa lỗi (ví dụ: trên Ubuntu 24.04 là 2:2.5-3ubuntu4.1).

+ Ngừng sử dụng Telnet: Do Telnet không mã hóa dữ liệu và có thiết kế không an toàn, khuyến nghị thay thế hoàn toàn bằng SSH.

3. Lỗ hổng bảo mật trên trình duyệt Chrome

3.1. CVE-2025-13630 – Type Confusion trong V8 JavaScript Engine – Lỗ hổng thực thi mã từ xa trong ứng dụng trình duyệt Chrome.

- Đánh giá mức độ nguy hiểm: Cao (điểm CVSS: 8.8/10).

- Mô tả kỹ thuật:

+ Lỗ hổng này xuất phát từ Type Confusion trong V8, thành phần xử lý JavaScript của Google Chrome. Kiểu "Type Confusion" xảy ra khi trình biên dịch nhầm lẫn kiểu đối tượng trong quá trình xử lý, dẫn tới truy cập bộ nhớ sai vị trí và có thể gây heap corruption. Khi heap bị hỏng, kẻ tấn công có thể lợi dụng để chạy mã tùy ý trong ngữ cảnh trình duyệt người dùng. Đây là lỗi thuộc CWE-843 - lỗi truy cập tài nguyên với kiểu dữ liệu không tương thích.

+ Tình huống khai thác: Tin tặc tạo một trang web chứa HTML/Javascript đặc biệt thiết kế để khai thác lỗi type confusion. Khi người dùng mở trang web này trong Chrome cũ, V8 xử lý đoạn mã bị lỗi, dẫn đến heap bị hỏng và cho phép mã độc được thực thi ngay trong tiến trình trình duyệt. Kết quả có thể là cookie và thông tin đăng nhập tài khoản web bị đánh cắp, trình duyệt bị chiếm quyền, hoặc mã độc tiếp tục được tải xuống.

- Phiên bản ảnh hưởng: Google Chrome phiên bản trước 143.0.7499.41.

- Khuyến nghị: Cập nhật Google Chrome lên phiên bản 143.0.7499.40/41 hoặc mới hơn, phiên bản đã vá lỗi này.

Link bản vá: https://chromereleases.googleblog.com/2025/12/stable-channel-update-for-desktop.html

3.2. CVE-2025-13631 – Inappropriate Implementation – Lỗ hổng leo thang đặc quyền cục bộ trong Google Updater

- Đánh giá mức độ nguy hiểm: Cao (điểm CVSS: 8.8/10).

- Mô tả kỹ thuật:

+ Lỗ hổng này bắt nguồn từ việc Google Updater, thành phần thực hiện cập nhật cho Google Chrome, xử lý không phù hợp các dữ liệu khi kiểm tra hoặc áp dụng bản cập nhật. Điều này dẫn tới khả năng leo thang đặc quyền cục bộ nếu file được thao túng bởi kẻ tấn công *(quyền thấp lên quyền cao)*.

+ Tình huống khai thác: Trong một môi trường mạng không an toàn, tin tặc theo dõi lưu lượng cập nhật Chrome và chặn kết nối tới server cập nhật thật. Sau đó cung cấp một bản cập nhật giả qua đường dẫn mạng. Do lỗ hổng kiểm tra tính toàn vẹn, Google Updater chấp nhận và chạy bản cập nhật giả. Điều này cho phép mã độc chạy với quyền cao hơn trên máy nạn nhân, có thể cài mã độc, công cụ gián điệp hoặc làm tiền đề cho các bước tấn công tiếp theo.

- Khuyến nghị: Cập nhật lên Chrome phiên bản 143.0.7499.40/41 hoặc phiên bản mới hơn để loại bỏ lỗi trong Updater.

Link bản vá: https://chromereleases.googleblog.com/2025/12/stable-channel-update-for-desktop.html

2.3. CVE-2025-13633 – Use-After-Free – Lỗ hổng thực thi mã từ xa trong Digital Credentials của Chrome

- Đánh giá mức độ nguy hiểm: Cao (điểm CVSS: 8.8/10).

- Mô tả kỹ thuật:

+ Lỗi này là kiểu use-after-free *(tiếp tục sử dụng một vùng nhớ đã bị giải phóng)* trong module Digital Credentials *(bộ phận quản lý các thông tin đăng nhập số như passkey và xác thực web)*. Lỗi xảy ra khi trình duyệt tiếp tục truy cập một vùng nhớ đã được giải phóng, làm sai lệch cấu trúc bộ nhớ (heap corruption). Tình trạng này có thể bị tin tặc lợi dụng để chèn và thực thi mã tùy ý trong tiến trình trình duyệt.

+ Tình huống khai thác: Kẻ tấn công gửi email hoặc tạo trang web chứa HTML được thiết kế để kích hoạt lỗi use-after-free khi Chrome xử lý thông tin xác thực số *(Digital Credentials)*. Khi người dùng truy cập liên kết này trong trình duyệt cũ, heap bị hỏng và mã do kẻ tấn công chèn sẵn chạy, có thể dẫn tới rò rỉ mật khẩu số hoặc chiếm đoạt thông tin đăng nhập vào tài khoản web.

- Khuyến nghị: Cập nhật lên Chrome phiên bản Chrome 143.0.7499.40/41 hoặc mới hơn.

Link bản vá: https://chromereleases.googleblog.com/2025/12/stable-channel-update-for-desktop.html

2.4. CVE-2026-1504 – Lỗ hổng bảo mật tồn tại trong API Background Fetch của trình duyệt Google

- Đánh giá mức độ nguy hiểm: Trung bình (điểm CVSS: 6.5/10).

- Mô tả kỹ thuật: Lỗi nằm ở việc triển khai không phù hợp (Inappropriate implementation) trong Background Fetch API. Kẻ tấn công có thể tạo một trang web độc hại để vượt qua chính sách đồng nguồn (Same-Origin Policy), từ đó rò rỉ hoặc đánh cắp dữ liệu (như cookies, token) từ các tab/trang web khác mà người dùng đang mở. Nguy cơ cao về việc xâm phạm quyền riêng tư và dữ liệu phiên làm việc của người dùng.

- Phiên bản ảnh hưởng: Các phiên bản Google Chrome trước 144.0.7559.110. Lỗ hổng này cũng ảnh hưởng đến các trình duyệt khác sử dụng nhân Chromium.

- Khuyến nghị: Nâng cấp trình duyệt lên phiên bản 144.0.7559.110 hoặc mới hơn.

2.5. CVE-2026-0899 - Lỗ hổng truy cập bộ nhớ ngoài phạm vi (Out-of-bounds memory access) trong công cụ V8 JavaScript engine của Google Chrome

- Đánh giá mức độ nguy hiểm: Cao (điểm CVSS: 8.8/10).

- Mô tả kỹ thuật: Kẻ tấn công từ xa có thể lừa người dùng truy cập vào một trang HTML được cấu trúc đặc biệt để khai thác lỗi tham chiếu bộ nhớ (object corruption). Điều này dẫn đến việc đọc hoặc ghi dữ liệu trái phép vào bộ nhớ, cho phép thực thi mã độc từ xa trong trình duyệt.

- Phiên bản ảnh hưởng: Các phiên bản Google Chrome trước 144.0.7559.110

- Khuyến nghị: Nâng cấp trình duyệt lên phiên bản 144.0.7559.110 hoặc mới hơn.

2.6. CVE-2026-0900 - Lỗ hổng triển khai không phù hợp (Inappropriate implementation) trong công cụ V8 JavaScript engine.

- Đánh giá mức độ nguy hiểm: Cao (điểm CVSS: 8.8/10).

- Mô tả kỹ thuật: Kẻ tấn công từ xa có thể lừa người dùng truy cập vào một trang HTML được chuẩn bị đặc biệt để khai thác lỗi object corruption (xâm phạm cấu trúc đối tượng). Việc khai thác thành công cho phép kẻ tấn công thực thi mã độc trong bộ nhớ, có khả năng dẫn đến việc chiếm quyền điều khiển trình duyệt hoặc truy cập dữ liệu nhạy cảm.

- Phiên bản ảnh hưởng: Các phiên bản Google Chrome trước 144.0.7559.59

- Khuyến nghị: Nâng cấp Google Chrome lên phiên bản mới nhất (khuyến nghị từ 144.0.7559.110 trở lên).

2.7. CVE-2026-0901 - Lỗ hổng đọc bộ nhớ ngoài phạm vi (Out-of-bounds Read) trong thành phần xử lý tệp tin đa phương tiện hoặc đồ họa của Chrome

- Đánh giá mức độ nguy hiểm: Cao (điểm CVSS: 8.1/10).

- Mô tả kỹ thuật: Kẻ tấn công có thể lừa người dùng mở một tệp tin hoặc truy cập trang web chứa nội dung đa phương tiện được cấu trúc đặc biệt để buộc trình duyệt đọc dữ liệu từ các vùng nhớ nhạy cảm không được phép. Điều này có thể dẫn đến việc rò rỉ thông tin bộ nhớ hệ thống hoặc gây ra tình trạng treo trình duyệt (DoS), tạo tiền đề cho các cuộc tấn công vượt rào bảo mật (bypass) tiếp theo.

- Phiên bản ảnh hưởng: Các phiên bản Google Chrome trước 144.0.7559.59

- Khuyến nghị: Nâng cấp Google Chrome lên phiên bản mới nhất (khuyến nghị từ 144.0.7559.110 trở lên).

4. Lỗ hổng bảo mật khác

4.1. CVE-2026-20119 - Lỗ hổng bảo mật tồn tại thiết bị mạng Cisco.

- Đánh giá mức độ nguy hiểm: Rất cao (điểm CVSS: 9.8/10).

- Mô tả kỹ thuật: Lỗ hổng nằm ở hệ thống con xử lý văn bản (Text Rendering Subsystem) của phần mềm Cisco TelePresence CE và Cisco RoomOS. Lỗi phát sinh do việc kiểm tra dữ liệu đầu vào không đầy đủ (Insufficient Validation). Kẻ tấn công từ xa, không cần xác thực, có thể gửi các yêu cầu chứa văn bản được chế tạo đặc biệt (ví dụ: một lời mời họp giả mạo). Khi thiết bị cố gắng hiển thị văn bản này, hệ thống sẽ bị lỗi và tự động khởi động lại (reload), gây ra tình trạng. Từ chối

dịch vụ (DoS). Đáng chú ý là cuộc tấn công không yêu cầu bất kỳ sự tương tác nào từ người dùng (không cần người dùng chấp nhận lời mời họp).

- Phiên bản ảnh hưởng: Cisco TelePresence Collaboration Endpoint (CE) Software. Cisco RoomOS Software (cả triển khai On-premises và Cloud). Các phiên bản 10, 11 và cũ hơn đều nằm trong diện ảnh hưởng.

- Khuyến nghị: Cập nhật phần mềm đối với thiết bị On-premises (nâng cấp lên phiên bản 11.27.5.0 hoặc 11.32.3.0); đối với triển khai Cloud (Cập nhật lên bản phát hành RoomOS October 2025 hoặc RoomOS December 2025).

4.2. CVE-2026-1642 - Lỗ hổng bảo mật tồn thiết mạng F5 NGINX

- Đánh giá mức độ nguy hiểm: Cao (điểm CVSS: 8.2/10).

- Mô tả kỹ thuật: Lỗ hổng nằm trong NGINX OSS và NGINX Plus khi được cấu hình làm proxy cho các máy chủ thượng nguồn (upstream) sử dụng giao thức TLS. Lỗi này thuộc loại chấp nhận dữ liệu không tin cậy đi kèm dữ liệu tin cậy. Một kẻ tấn công ở vị trí trung gian (Man-in-the-Middle - MITM) giữa NGINX và máy chủ thượng nguồn có thể chèn các dữ liệu văn bản thuần túy (plain text) vào phản hồi từ máy chủ thượng nguồn trước khi nó được gửi tới khách hàng (client). Điều này cho phép kẻ tấn công giả mạo hoặc thay đổi nội dung phản hồi mà người dùng nhận được.

- Phiên bản ảnh hưởng:

+ NGINX Plus: Các nhánh từ R32 đến R36 P1.

+ NGINX Open Source: Các phiên bản từ 1.3.0 đến 1.29.4.

+ NGINX Ingress Controller: Phiên bản 5.x (5.0.0 - 5.3.2).

+ NGINX Gateway Fabric: Phiên bản 2.x (2.0.0 - 2.4.0).

- Khuyến nghị: Cập nhật phần mềm:

+ NGINX Plus: Nâng cấp lên R36 P2, R35 P1, hoặc R32 P4.

+ NGINX Open Source: Nâng cấp lên 1.29.5 hoặc 1.28.2.

+ NGINX Ingress Controller: Nâng cấp lên 5.3.3.

4.3. CVE-2026-0755 - Lỗ hổng bảo mật ứng dụng Gemini MCP Tool

- Đánh giá mức độ nguy hiểm: Rất cao (điểm CVSS: 9.8/10).

- Mô tả kỹ thuật: Lỗ hổng bắt nguồn từ cách Gemini MCP Tool triển khai phương thức execAsync. Hàm này được sử dụng để thực thi các lệnh hệ thống theo cơ chế bất đồng bộ, nhưng lại không kiểm tra và làm sạch đầy đủ dữ liệu đầu vào do người dùng cung cấp. Lỗ hổng này cho phép kẻ tấn công từ xa thực thi mã tùy ý trên hệ thống mục tiêu mà không cần xác thực hay tương tác từ phía người dùng.

- Phiên bản ảnh hưởng: Tất cả các phiên bản gemini-mcp-tool đang lưu hành tính đến tháng 1/2026.

- Khuyến nghị: Vì đây là lỗ hổng Zero-day chưa có bản vá, bạn nên thực hiện các biện pháp phòng vệ cấp bách sau:

+ Cô lập mạng ngay lập tức: Ngắt kết nối hoặc hạn chế tối đa việc truy cập công cụ này từ mạng Internet công cộng.

+ Thiết lập Access Control: Chỉ cho phép truy cập từ các mạng nội bộ tin cậy.

+ Cân nhắc giải pháp thay thế: Xem xét việc tạm ngừng sử dụng hoặc chuyển sang công cụ khác cho đến khi nhà cung cấp tung ra bản vá lỗi.

4.4. CVE-2026-20803 - Lỗ hổng bảo mật tồn tại SQL Server

- Đánh giá mức độ nguy hiểm: Cao (điểm CVSS: 7.2/10).

- Mô tả kỹ thuật: Lỗ hổng thiếu xác thực cho chức năng quan trọng (Missing Authentication for Critical Function). Lỗi này cho phép một kẻ tấn công đã được xác thực (với quyền hạn cao - PR:H) có thể khai thác qua môi trường mạng để thực hiện các chức năng nhạy cảm mà không cần trải qua các bước kiểm tra danh tính bổ sung. Điều này dẫn đến khả năng leo thang đặc quyền (Privilege Escalation), cho phép kẻ tấn công kiểm soát hoàn toàn tính toàn vẹn và tính bảo mật của cơ sở dữ liệu.

- Phiên bản ảnh hưởng: Các phiên bản SQL Server 2022 dưới 16.0.1165.1.

- Khuyến nghị: Cập nhật ngay bản vá KB5073031 (đưa SQL Server 2022 lên bản build 16.0.1165.1). Hạn chế quyền sysadmin, chỉ cấp cho nhân sự thực sự cần thiết và giám sát chặt chẽ các lệnh thực thi hệ thống.

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, kịp thời cập nhật, vá lỗi hệ thống nếu phát hiện tồn tại các lỗ hổng trên, 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);
- Phòng Tham mưu;
- Lưu: VT, ANM.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CÔNG AN TỈNH QUẢNG NGÃI

Đại tá Võ Văn Dương