BỘ CÔNG AN
CÔNG AN TỈNH HÀ TĨNH

Số: 387/CAT-ANM

V/v thông báo lỗ hổng bảo mật nghiêm trọng tháng 01/2026

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

Hà Tĩnh, ngày 30 tháng 01 năm 2026

Kính gửi:
- Các Ban Đảng, UBKT, Văn phòng Tỉnh ủy;
- Các Đảng ủy trực thuộc Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các sở, ban, ngành, đoàn thể cấp tỉnh;
- Các doanh nghiệp nhà nước trên địa bàn tỉnh;
- Đảng ủy, UBND cấp xã.

Tháng 01/2026 trên không gian mạng xuất hiện nhiều chiến dịch tấn công mạng tinh vi và các lỗ hổng nghiêm trọng trên các phần mềm ứng dụng phổ biến. Đặc biệt hệ thống quản trị mã độc tập trung ghi nhận một số loại mã độc nguy hiểm đang lây nhiễm, ảnh hưởng trực tiếp đến các cơ quan, đơn vị trên địa bàn tỉnh. Các loại virus, mã độc này có thể bị đối tượng tấn công lợi dụng để chiếm quyền điều khiển hệ thống, đánh cắp và mã hóa dữ liệu đòi tiền chuộc (ransomware). Công an tỉnh thông báo thông tin và hướng dẫn giải pháp khắc phục như sau:

1. Các nguy cơ tấn công mạng và lỗ hổng bảo mật nghiêm trọng

1.1. Cảnh báo lỗ hổng nghiêm trọng thực thi mã từ xa trong dịch vụ cổng máy tính từ xa của Microsoft (Remote Desktop Gateway)

- Mức độ: Đặc biệt nghiêm trọng.

- Mô tả: Lỗ hổng tồn tại trong các dịch vụ cổng máy tính từ xa (Remote Desktop Gateway) xử lý các kết nối đến. Lỗ hổng này cho phép đối tượng tấn công từ bên ngoài Internet, không cần xác thực, có thể gửi một gói tin được chế tạo đặc biệt đến máy chủ và thực thi mã độc từ xa với quyền quản trị cao nhất. Khai thác thành công lỗ hổng này đồng nghĩa với việc đối tượng có thể chiếm quyền điều khiển hoàn toàn máy chủ cổng và từ đó xâm nhập sâu vào toàn bộ hệ thống mạng nội bộ của cơ quan, đơn vị.

- Phiên bản ảnh hưởng: Windows Server 2019, Windows Server 2022.

- Giải pháp khắc phục: (1) Đối với quản trị viên các hệ thống khẩn trương rà soát các máy chủ đang cài đặt dịch vụ Remote Desktop Gateway và cập nhật ngay bản vá bảo mật tháng 01/2026 của Microsoft. (2) Đối với các đơn vị chưa thể cập nhật ngay tạm thời áp dụng biện pháp giảm thiểu rủi ro bằng cách cấu hình tường lửa, chỉ cho phép các địa chỉ IP tin cậy được phép kết nối đến cổng dịch vụ 3391/UDP của máy chủ Remote Desktop Gateway.

1.2. Cảnh báo chiến dịch tấn công lừa đảo có chủ đích sử dụng công nghệ giả mạo giọng nói (Deepfake Voice)

- Mức độ: Rất nghiêm trọng.

- Mô tả: Các đối tượng lừa đảo thu thập thông tin về cơ cấu tổ chức của các cơ quan, đặc biệt nhắm vào bộ phận kế toán, tài chính. Sau đó chúng sử dụng công nghệ Trí tuệ nhân tạo (AI) để giả mạo giọng nói của lãnh đạo đơn vị, thực hiện các cuộc gọi qua Zalo, Whatsapp... đến cán bộ kế toán. Với kịch bản khẩn cấp (như "Anh/chị đang đi công tác đột xuất, cần chuyển gấp một khoản tiền cho đối tác...") các đối tượng sẽ yêu cầu chuyển tiền vào một tài khoản do đối tượng chỉ định. Do giọng nói giống hệt nên nhiều người đã mất cảnh giác và làm theo.

- Giải pháp khắc phục: (1) Quán triệt quy trình xác thực: Tuyệt đối không thực hiện bất kỳ giao dịch chuyển tiền nào chỉ dựa trên một cuộc gọi điện thoại hoặc gọi qua ứng dụng OTT, kể cả khi nhận ra đó là giọng nói của lãnh đạo. Phải thiết lập và tuân thủ nghiêm ngặt quy trình xác thực đa kênh như gọi lại vào số điện thoại chính thức của lãnh đạo, nhắn tin qua kênh liên lạc khác hoặc yêu cầu có văn bản chỉ đạo hợp lệ trước khi thực hiện giao dịch. (2) Nâng cao nhận thức bằng cách phổ biến rộng rãi thủ đoạn lừa đảo mới này đến toàn thể cán bộ, công chức, viên chức, đặc biệt là những người làm công tác tài chính, kế toán.

1.3. Lỗ hổng trong các phần mềm kế toán phổ biến cho phép đánh cắp dữ liệu

- Mức độ: Nghiêm trọng.

- Mô tả: Lỗ hổng bảo mật được phát hiện trong module đồng bộ hóa dữ liệu của một số phần mềm kế toán doanh nghiệp đang được sử dụng rộng rãi. Lỗ hổng này cho phép tin tặc, nếu có cùng lớp mạng, có thể gửi các truy vấn độc hại để trích xuất toàn bộ cơ sở dữ liệu kế toán của đơn vị mà không cần có tài khoản đăng nhập. Việc này dẫn đến nguy cơ rò rỉ toàn bộ thông tin tài chính, dữ liệu nhân sự, thông tin khách hàng, đối tác.

- Phiên bản ảnh hưởng: Các phiên bản phần mềm kế toán MISA, FAST... chưa được cập nhật bản vá cuối tháng 12/2025.

- Giải pháp khắc phục: (1) Đối với bộ phận kế toán liên hệ ngay lập tức với nhà cung cấp phần mềm (MISA, FAST...) để yêu cầu và thực hiện việc cập nhật phiên bản phần mềm mới nhất. (2) Đối với quản trị mạng rà soát, cấu hình tường lửa để giới hạn nghiêm ngặt các kết nối đến máy chủ kế toán, chỉ cho phép các máy tính được chỉ định trong mạng nội bộ được phép truy cập.

2. Cảnh báo nghiêm trọng thông qua hệ thống quản trị mã độc tập trung EDR trên địa bàn tỉnh

2.1. Cảnh báo mã độc lây lan Worm.VBS.Dinihou.r

- Mức độ: Nghiêm trọng.

- Mô tả: Worm.VBS.Dinihou.r là mã độc dạng worm được viết bằng ngôn ngữ VBScript (VBS), có khả năng tự động lây lan thông qua các thiết bị lưu trữ di động (USB), thư mục chia sẻ mạng và các tệp tin có đuôi giả mạo. Mã độc thường ngụy trang dưới dạng các tệp tin quen thuộc để đánh lừa người dùng mở thực thi. Sau khi xâm nhập thành công, mã độc tạo và chỉnh sửa các tập tin hệ thống, thay đổi khóa Registry nhằm duy trì hoạt động khi hệ thống khởi động. Đồng thời Worm.VBS.Dinihou.r có thể tải thêm mã độc khác từ Internet, làm gia tăng nguy cơ bị kiểm soát hệ thống và mất an toàn thông tin[1].

- Giải pháp khắc phục: (1) Đối với quản trị viên hệ thống cần rà soát các máy tính bị lây nhiễm mã độc bằng phần mềm Smart IR để kịp thời xử lý; kiểm tra và vô hiệu hóa các tập tin VBS nghi vấn, đặc biệt trong thư mục hệ thống và các thiết bị lưu trữ di động. (2) Đối với người dùng thực hiện quét virus trước khi mở USB, mở tài liệu; luôn bật phần mềm diệt virus Smart IR.

2.2. Cảnh báo mã độc lây nhiễm qua file Excel (Virus.MSExcel.Laroux-based)

- Mức độ: Nghiêm trọng.

- Mô tả: Đây là loại macro-virus lây lan qua các file Microsoft Excel, đặc biệt phát tán mạnh qua ứng dụng Zalo. Khi người dùng mở file và bật tính năng "cho phép Macros" (Enable Macros) virus sẽ lây nhiễm vào hệ thống, có khả năng đánh cắp thông tin nhạy cảm và là tiền đề cho các cuộc tấn công mã hóa tống tiền (ransomware)[2].

- Giải pháp khắc phục: (1) Đối với quản trị viên hệ thống cần cấu hình Group Policy để vô hiệu hóa hoặc cảnh báo nghiêm ngặt việc thực thi macro trong các văn bản Office. (2) Đối với người dùng tuyệt đối không bấm "cho phép

---

[1] Ghi nhận lây nhiễm tại: Xã Tùng Lộc; Xã Kim Hoa.

[2] Ghi nhận lây nhiễm tại: Xã Nghi Xuân; Xã Đan Hải; Xã Sơn Hồng; Phường Sông Trí; Xã Sơn Kim 2; Xã Sơn Kim 1; Phường Bắc Hồng Lĩnh; Xã Sơn Giang; Xã Sơn Tây; Xã Sơn Giang|Trường THCS Hải Thượng Lãn Ông; Sở Tài chính|Văn phòng Sở Tài chính; Xã Đông Kinh; Xã Mai Hoa|Trường Mầm non Đức Lĩnh; Sở Xây dựng; Xã Yên Hòa; Xã Kỳ Xuân; Sở Khoa học công nghệ; Sở Y tế|Chi cục Dân số; Sở Công thương|Văn phòng Sở công thương; Sở Văn hoá Thể thao và Du lịch|Trung tâm Văn hoá Truyền thông Hương Sơn; Xã Tứ Mỹ; Xã Hương Bình; Phường Trần Phú|Đảng uỷ-UBND-MTTQ; Sở Y tế|Trung tâm y tế Hương Sơn; Xã Hương Sơn; Xã Lộc Hà; Xã Sơn Tiến; Xã Sơn Kim 1|Trường Tiểu học Sơn Kim 1; Xã Thạch Hà|Trung tâm chính trị; Phường Thành Sen|Trường Mầm non Thạch Quý; Sở Nông nghiệp và Môi trường|Văn phòng Đăng ký đất đai Thị xã Hồng Lĩnh; Xã Kỳ Anh; Xã Kim Hoa; Sở Y tế|Trung tâm Kiểm nghiệm thuốc mỹ phẩm thực phẩm; Xã Cẩm Duệ; Phường Nam Hồng Lĩnh; Xã Xuân Lộc; Xã Tiên Điền; Xã Đông Kinh|UBND-Đảng uỷ-MTTQ-TTHCC xã Đông Kinh; Phường Hải Ninh; Xã Cổ Đạm|Trường Tiểu học Cổ Đạm; Xã Đức Quang; Sở Nông nghiệp và Môi trường|Trung tâm nước sạch và vệ sinh môi trường nông thôn; Sở Nông nghiệp và Môi trường|Vườn Quốc gia Vũ Quang; Xã Mai Phụ; Xã Cẩm Lạc; Sở Nông nghiệp và Môi trường|Trung tâm quan trắc và tài nguyên môi trường; Xã Hương Sơn|Trường THCS Trung Phú; Xã Sơn Tiến|Trường THCS Nguyễn Khắc Viện; Sở Giáo dục và Đào tạo|Văn phòng Sở giáo dục và Đào tạo; Sở Văn hoá Thể thao và Du lịch|Trung tâm Văn hoá Truyền thông Vũ Quang; Sở Y tế|Trung tâm y tế Tiên Điền; Xã Gia Hanh; Xã Cổ Đạm; Xã Sơn Kim 2|Trường Tiểu học Sơn Kim 2; Xã Sơn Giang|Trường Tiểu học Quang Diệm; Xã Sơn Hồng|Trường Tiểu học Sơn Hồng; Công an tỉnh|Công an phường Hà Huy Tập; Xã Đồng Lộc; Sở Y tế|Bệnh viện Sức khỏe Tâm thần; Sở Giáo dục và Đào tạo|THPT Phan Đình Phùng; Xã Kim Hoa|Trường THCS Phan Đình Phùng; Thanh tra tỉnh; Phường Thành Sen|UBND phường Thành Sen; Phường Thành Sen|Đảng uỷ-MTTQ phường Thành Sen; Xã Thạch Hà|UBND-Đảng uỷ-MTTQ-TTHCC; Xã Đức Minh; Xã Cẩm Xuyên; Xã Đức Thọ; Xã Hương Xuân; Xã Tùng Lộc; Xã Trường Lưu; Xã Thạch Lạc; Xã Đức Đồng; Xã Việt Xuyên; Xã Vũ Quang; Xã Thạch Xuân; Xã Kỳ Văn; Xã Hồng Lộc; Xã Đồng Tiến|UBND-Đảng uỷ-MTTQ-TTHCC xã Đồng Tiến; Xã Thạch Khê|UBND-Đảng uỷ-MTTQ-TTHCC xã Thạch Khê; Sở Y tế|Trung tâm công tác xã hội.

nội dung hoạt động" (Enable Content) hoặc "cho phép Macros" (Enable Macros) đối với các tệp tin nhận được từ nguồn không tin cậy và luôn bật phần mềm diệt virus Smart IR.

2.3. Cảnh báo mã độc lây nhiễm qua file AutoCAD (Virus.Acad.Bursted.a, Trojan.Acad.Agent.a)

- Mức độ: Nghiêm trọng.

- Mô tả: Đây là loại virus lây nhiễm vào môi trường làm việc của phần mềm AutoCAD. Khi người dùng mở một tệp bản vẽ bất kỳ, mã độc sẽ được kích hoạt và có khả năng đánh cắp, phá hoại các bản vẽ thiết kế, dữ liệu quy hoạch, dự án quan trọng[3].

- Giải pháp khắc phục: (1) Đối với quản trị viên hệ thống cần rà soát các máy tính có cài đặt AutoCAD. Sử dụng phần mềm diệt virus để làm sạch. Kiểm tra và xóa các tệp tin độc hại (như acad.lsp, acaddoc.lsp) trong thư mục cài đặt và thư mục người dùng của AutoCAD. (2) Đối với người dùng không mở các file bản vẽ không rõ nguồn gốc, báo cáo ngay cho bộ phận công nghệ thông tin khi phần mềm AutoCAD có các biểu hiện bất thường và luôn bật phần mềm diệt virus Smart IR.

2.4. Phát hiện một số file .exe tại các đơn vị ghi nhận hành vi nguy hiểm có thể dẫn đến tấn công mã hóa dữ liệu trong tương lai

- Mức độ: Rất nghiêm trọng.

- Mô tả: Một số tệp tin thực thi (.exe) tại các đơn vị có hành vi nguy hiểm, tiềm ẩn rủi ro cao đối với hệ thống thông tin. Các tệp tin này có thể được phát tán thông qua email, ứng dụng nhắn tin (Zalo, Telegram...), thiết bị lưu trữ USB hoặc tải về từ Internet.

Khi người dùng vô tình thực thi (chạy) các file .exe, mã độc có thể được kích hoạt, cho phép kẻ tấn công xâm nhập hệ thống, tải thêm mã độc khác, duy trì quyền kiểm soát, và đặc biệt là tiền đề cho các cuộc tấn công mã hóa dữ liệu tống tiền (ransomware) trong tương lai[4].

- Giải pháp khắc phục: (1) Đối với quản trị viên hệ thống cần rà soát, kiểm tra và loại bỏ ngay các file .exe không rõ nguồn gốc trên máy trạm và máy chủ. Cấu hình Group Policy hoặc các giải pháp Endpoint Security để hạn chế hoặc chặn việc thực thi file .exe từ các thư mục không an toàn (Downloads, Temp, USB...). Triển khai và cập nhật đầy đủ phần mềm diệt virus Smart IR cho hệ thống. (2) Đối với người dùng cần tuyệt đối không mở hoặc chạy các file .exe nhận được từ email, ứng dụng nhắn tin hoặc nguồn không rõ ràng. Không tải và cài đặt phần mềm, công cụ, file crack hoặc keygen từ Internet. Luôn bật

---

[3] Ghi nhận lây nhiễm tại: Sở Xây dựng; Xã Can Lộc; Phường Hà Huy Tập; Phường Hải Ninh.

[4] Ghi nhận lây nhiễm tại: Xã Cẩm Duệ; Xã Hà Linh|Trường THCS Hà Linh; Văn phòng Đoàn ĐBQH và HĐND tỉnh; Xã Can Lộc; Xã Can Lộc|Trường THCS Xuân Diệu; Xã Trường Lưu; Sở Công thương|Văn phòng Sở công thương; Sở Giáo dục và Đào tạo|THPT Nguyễn Văn Trỗi; Xã Hồng Lộc; Sở Nông nghiệp và Môi trường|Văn phòng Đăng ký đất đai tỉnh; Sở Y tế|Trung tâm y tế Hồng Lĩnh; Sở Tài chính|Văn phòng Sở Tài chính.

phần mềm diệt virus Smart IR, kịp thời báo cáo bộ phận công nghệ thông tin khi phát hiện cảnh báo bất thường.

2.5. Phát hiện một số Trang thông tin điện tử hiện vẫn sử dụng giao thức HTTP

- Mức độ: Rất nghiêm trọng.

- Mô tả: Qua công tác rà soát, kiểm tra an toàn thông tin, phát hiện một số Trang thông tin điện tử hiện vẫn sử dụng giao thức HTTP, do chưa được triển khai và kích hoạt chứng thư số SSL/TLS cho máy chủ Web. Việc sử dụng giao thức HTTP khiến dữ liệu trao đổi giữa người dùng và máy chủ không được mã hóa, tiềm ẩn nguy cơ bị nghe lén, đánh cắp hoặc chỉnh sửa nội dung trong quá trình truyền tải (tấn công Man-in-the-Middle). Tình trạng này không đáp ứng các khuyến nghị và yêu cầu hiện hành về bảo đảm an toàn thông tin, đặc biệt đối với các hệ thống cung cấp dịch vụ công hoặc có chức năng thu thập thông tin người dùng[5].

- Giải pháp khắc phục: (1) Đối với quản trị viên hệ thống cần khẩn trương triển khai và kích hoạt chứng thư số SSL/TLS hợp lệ cho máy chủ Web từ các tổ chức cung cấp chứng thực uy tín. Cấu hình chuyển hướng bắt buộc từ HTTP sang HTTPS, vô hiệu hóa hoàn toàn truy cập HTTP sau khi triển khai thành công. (2) Đối với người dùng chỉ truy cập và sử dụng dịch vụ khi trang Web hiển thị HTTPS và biểu tượng ổ khóa an toàn trên trình duyệt. Không nhập thông tin đăng nhập, thông tin cá nhân trên các trang Web sử dụng giao thức HTTP.

Khi phát hiện dấu hiệu tấn công mạng đề nghị các đơn vị, địa phương liên hệ Công an tỉnh (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, số điện thoại: 099.338.6777) để được phối hợp, hỗ trợ xử lý.

Công an tỉnh thông báo các đơn vị, địa phương biết, đề nghị khẩn trương rà soát, xử lý các virus, mã độc và các lỗ hổng bảo mật trên hệ thống. Giao Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao rà soát các đơn vị, địa phương không triển khai khắc phục các tồn tại, hạn chế đã được Công an tỉnh thông báo từ các kỳ trước, tham mưu giải pháp xử lý theo quy định./.

Nơi nhận:
- Như trên;
- Đ/c Giám đốc (để báo cáo);
- Lưu: VT, ANM.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ X.H.C.N VIỆT NAM
CÔNG AN TỈNH HÀ TĨNH

Thượng tá Nguyễn Quốc Hùng

[5] Ghi nhận một số trang như: http://sotaichinh.hatinh.gov.vn/; http://thcskythinh.thixakyanh.edu.vn/; http://ubmttq.hatinh.gov.vn/; http://cdc.hatinh.gov.vn/; http://tuphap.hatinh.gov.vn/ (đề nghị các đơn vị triển khai theo khuyến nghị và báo cáo về Công an tỉnh kết quả thực hiện).