ỦY BAN NHÂN DÂN **XÃ THẠCH HÀ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:402 /UBND-VP V/v thông báo lỗ hổng bảo mật nghiêm trọng tháng 01, 02/2026	*Thạch Hà, ngày 25 tháng 3 năm 2025*

Kính gửi:

- Đảng ủy, HĐND, UBND, UBMTTQ Việt Nam xã;
- Trung tâm Chính trị xã;
- Các phòng, ban, đơn vị cấp xã;
- Các Trường học trên địa bàn xã;
- Các Thôn, Tổ chuyển đổi số cộng đồng trên địa bàn xã.

Thực hiện Văn bản số 387/CAT-ANM ngày 30/01/2026 của Công an tỉnh về việc thông báo lỗ hổng bảo mật nghiêm trọng tháng 01/2026; Công văn số 785/CAT-ANM ngày 05/3/2026 của Công an tỉnh về việc thông báo lỗ hổng bảo mật nghiêm trọng tháng 02/2026.

Theo Công văn trong tháng 01 và 02 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 tới 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 kiển hệ thống, đánh cắp và mã hóa dữ liệu đòi tiền chuộc (ransomware). Trên địa bàn xã Thạch Hà ghi nhận 02 Cảnh báo nghiêm trọng thông qua hệ thống quản trị mã độc tập trung EDR như sau:

1. 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)[1].

- Giải pháp khắc phục:

+ 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.

[1] Ghi nhận lây nhiễm tại: Đảng ủy, Trung tâm chính trị, UBND, MTTQ và Trung tâm phục vụ Hành chính công

+ Đối với người dùng: tuyệt đối không bấm "cho phép nội dung hoạt động" (Enable Content) hoặc "Cho phép Macros" (Enable Macros) đối với tệp tin nhận được từ nguồn không tin cậy và luôn bật phần mềm diệt virus Smart IR.

2. 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.

- Giải pháp khắc phục:

+ Đối với quản trị viên hệ thống: cần rà soát các mát 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.

+ Đối với người dùng: không mở các file bản vẽ không rõ nguồn gốc, báo cáo ngay cho cán bộ phụ trách CNTT khi phần mềm AutoCAD có các biểu hiện bất thường và luôn bật phần mềm diệt virus Smart IR.

Ngoài 02 cảnh báo nghiêm trọng ghi nhận lây nhiễm tại Thạch Hà. Trên địa bàn tỉnh cũng ghi nhận một số cảnh báo nghiêm trọng thông qua hệ thống quản trị mã độc tập trung EDR và nguy cơ tấn công mạng, lỗ hổng bảo mật nghiêm trọng (có văn bản gửi kèm). Đề nghị các Cán bộ, Công chức, Viên chức nghiên cứu.

Khi phát hiện có dấu hiệu tấn công mạng đề nghị các phòng, ban, ngành, đơn vị và các cá nhân 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.

UBND xã thông báo các phòng, ban, đơn vị biết, cảnh giác và nghiêm túc thực hiện các chế độ bảo mật./.

Nơi nhận:
- Như trên;
- Chủ tịch, các PCT UBND xã;
- Công an xã;
- Lưu: VT, VP.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

U.B.N.D XÃ THẠCH HÀ T. HÀ TĨNH

Mai Văn Dũng