XUẤT HIỆN MÃ ĐỘC TẤN CÔNG LỖI WINDOWS HELP

Micros

Microsoft cho biết đang điều tra thêm về lỗ hổng bảo mật tệp tin Windows Help mới được phát hiện đồng thời cảnh báo mã độc tấn công lỗi này đã xuất hiện trên Internet.

Thực tế lỗi này đã được McAfee phát hiện và thông báo cho Microsoft từ ngày 11/4 cùng với 3 lỗi được xem là zero-day khác trong Office. Ngay sau đó Microsoft đã lên tiếng phủ nhận 3 lỗi zero-day đồng thời phát đi cảnh báo về lỗi Windows Help.

Lỗi tệp tên Windows Help thực chất là một lỗi bảo mật tràn bộ nhớ đệm. Lỗi này tồn tại trong Windows XP, Windows Server 2003, Windows NT và Windows 2000.

Hãng bảo mật Security Focus cho biết lỗi này phát sinh khi ứng dụng Help File Viewer không thể thực hiện kiểm tra biên bộ nhớ trước khi sao chép dữ liệu sang bộ nhớ đệm. Lỗi xảy ra nếu ứng dụng phải xử lý một tệp tin Windows Help độc hại.

"Nếu khai thác thành công lỗi bảo mật tin tặc có thể giành được quyền thực thi mã lệnh trên hệ thống mắc lỗi. Còn nếu không thành công thì chúng cũng gây ra một vụ tấn công từ chối dịch vụ," Security Focus cho biết.

Người phát ngôn của Microsoft khẳng định hãng đang điều tra thêm về lỗ hổng này đồng thời khẳng định từ trước đến nay Microsoft luôn xem tệp tin Windows Help là một chuẩn định dạng nguy hiểm tương tự "exe". Hãng khuyến cáo người dùng không nên mở những tệp tin này ra nếu chúng được gửi đến từ một nguồn không rõ ràng.

Phát biểu trên trang blog của mình, ông Hon Lau - một chuyên gia của Security Response Team của Symantec - cho biết hiện chưa có vụ tấn công nào nhắm mục tiêu vào lỗi Windows Help và phát tán rộng.

Tuy nhiên, ông Lau cũng cho biết hiện đã xuất hiện mã độc có tên Bloodhound.Exploit.135 có khả năng tấn công lỗi Windows Help. Mã độc này đã được phát tán trên mạng Internet.

Hoàng Dũng