TẠP CHÍ ĐIỆN TỬ
THƯƠNG HIỆU & CÔNG LUẬN

Cảnh báo lỗ hổng nguy hiểm gây ảnh hưởng tới 1 triệu máy chủ

16:00 06/03/2020

Đây là lỗ hổng trên phần mềm mã nguồn mở Apache Tomcat. Lỗ hổng này có thể ảnh hưởng tới hơn 1 triệu máy chủ đang hoạt động trên thế giới, trong đó có Việt Nam.

Mới đây, các chuyên gia an ninh mạng tạiViệt Nam đã lên tiếng cảnh báo về lỗ hổng Ghostcast trên phần mềm mã nguồn mở Apache Tomcat. Lỗ hổng này cho phép kẻ tấn công có thể đọc các tệp tin cấu hình của ứng dụng, đánh cắp mật khẩu hoặc API token, thậm chí chiếm quyền điều khiển máy chủ.

Ghostcat là một lỗ hổng trong giao thức AIP Tomcat (Apache JServ Protocol)



ực sử

Một lỗ hổng trong phần mềm mã nguồn mở Apache Tomcat vừa được phát hiện

Tuy là phần mềm miễn phí, thế nhưng Apache Tomcat được đánh giá cao bởi khả năng thiết lập môi trường website an toàn, tiết kiệm chi phí và tính hiệu quả cao. Hiện nay, Apache Tomcat đang chiếm gần 50% thị phần website trên thế giới.

Apache TomCat luôn nằm trong danh sách những phần mềm mã nguồn mở phổ biến nhất hiện nay trên thế giới và được sử dụng rộng rãi bởi rất nhiều các đơn vị trong lĩnh vực tài chính, ngân hàng, viễn thông... Do đó, việc xuất hiện lỗ hổng trên phần mềm này được đánh giá là cực kỳ nguy hiểm.

Lỗ hổng GhostCat có mã theo dõi CVE-2020-1938 (CVSS 9.8). Lỗ hổng này được tin tặc khai thác dưới dạng chèn ký tự đặc biệt trong lúc gửi những yêu cầu tới máy chủ để đọc mã nguồn hoặc các thông tin file cấu hình máy chủ. Khi nắm được các file cấu hình này, tin tặc có thể tiếp cận và cài đặt backdoor để chiếm quyền điều khiển từ xa và thực thi các cuộc tấn công mạng khác.

Theo các chuyên gia, lỗ hổng Ghostcat hiện đã được phát hiện trên tất cả các phiên bản (9.x/8.x/7.x/6.x) của Apache Tomcat phát hành trong suốt 13 năm qua. Điều đặc biệt nghiêm trọng là các mã khai thác đã xuất hiện và được chia sẻ tràn lan trên Internet, từ đó các tin tặc có thể tìm kiếm và triển khai các phương thức xâm nhập vào máy chủ web một cách dễ dàng.

Thống kê của công cụ tìm kiếm lỗ hổng BinaryEdge cho thấy, hiện nay có hơn một triệu máy chủ Tomcat hiện đang hoạt động, do đó các chuyên gia nhấn mạnh rằng, tất cả doanh nghiệp, cá nhân sử dụng Apache Tomcat không phải phiên bản mới nhất đều nằm trong danh sách có thể trở thành con mồi của kẻ tấn công.

Theo khuyến cáo của giới chuyên môn, các doanh nghiệp sử dụng hệ thống Apache Tomcat cần cập nhật hệ thống lên phiên bản mới nhất và không bao giờ mở cổng AJP đến các máy Client không đáng tin cậy.

Đội ngũ của Tomcat cũng cho biết: “Người dùng nên lưu ý một thay đổi đã được thực hiện trong cấu hình AJP Connector mặc định phiên bản 9.0.31. Do vậy, người dùng cập nhật lên phiên bản 9.0.31 hoặc cao hơn sẽ cần phải thực hiện những thay đổi nhỏ trong cấu hình của mình.”.

Nếu không thể nâng cấp phiên bản máy chủ bị ảnh hưởng ngay lập tức, người dùng có thể khắc phục tạm thời bằng cách tắt AJP Connector, hoặc chuyển hướng nó về một cổng cục bộ để tránh những rủi ro không đáng có tới máy chủ.

Theo Vietnamnet