VNPT Cyber Immunity

DỊCH VỤ CỦA VNPT

GIẢI PHÁP BẢO MẬT CHO THIẾT BỊ IOT VNPT IOT GUARD

GIỚI THIỆU

VNPT IoT Guard là giải pháp phát hiện và ngăn chặn xâm nhập thiết bị IoT cho phép bảo vệ thiết bị IoT chống các loại virus, mã độc; hỗ trợ truy vấn, điều tra nguyên nhân và ứng cứu kịp thời khi có sự cố về an toàn thông tin; ngăn chặn các cuộc tấn công, khai thác lỗ hổng phần mềm lên thiết bị.

LỢI ÍCH NỔI BẬT

01 Giám sát và lọc tất cả các thao tác từ phần mềm tác động đến phần cứng.

02 Ngăn chặn khai thác lỗ hổng phần mềm chưa được biết đến (0-day).

03 Ngăn chặn mã độc lây lan giữa các thiết bị IoT.

04 Trích xuất nhật ký các thiết bị, trích xuất bộ nhớ thiết bị khi có cảnh báo bị khai thác lỗ hổng phục vụ công tác điều tra, phát hiện lỗ hổng 0day.

05 Cập nhật RULE, firmware qua server điều khiển tập trung.

VNPT Cyber Immunity

CÁC TÍNH NĂNG CHÍNH

Thiết bị IoT xuất hiện càng ngày càng nhiều và đóng vai trò quan trọng trong cuộc sống hiện đại từ việc mở khóa cửa ở các ngôi nhà thông minh đến xử lý dữ liệu của các cảm biến trong nhà máy hạt nhân, các thiết bị này có đặc điểm nhỏ gọn, khả năng xử lý không quá cao, nên thường không tích hợp được các mã nguồn mở hiện đại dẫn đến tồn tại nhiều lỗ hổng nguy hiểm. VNPT IoT là giải pháp giúp hạn chế tối đa khả năng xâm nhập, khai thác các thiết bị IoT, đồng thời trích xuất nhật ký, bộ nhớ thiết bị khi có cảnh báo khai thác, nhằm kịp thời ngăn chặn vá lỗ hổng 0day đang bị khai thác.

01 NHÓM CHỨC NĂNG GIÁM SÁT BẤT THƯỜNG

Thu thập thông tin, giám sát sự kiện an toàn thông tin

- Giám sát các lệnh thao tác đến hệ thống file.
- Giám sát các lệnh thao tác phân vùng ổ cứng.
- Giám sát các lệnh thao tác đến các phần mềm khác.
- Giám sát các lệnh thao tác đến kết nối mạng.

Ngăn chặn xâm nhập

Cơ chế Whitelist, chỉ cho phép thực thi các lệnh sạch của chính hệ thống IoT. Các lệnh khác sẽ được xem là độc hại và bị ngăn chặn. Đây là cơ chế tối ưu nhất tuy nhiên sẽ mất nguồn lực để liệt kê danh sách các lệnh sạch. Cơ chế Blacklist, ngăn chặn các lệnh phổ biến khi bị kẻ xấu tấn công, mà không cần phải liệt kê toàn bộ lệnh sạch của hệ thống, giảm thiểu nguồn lực để xây dựng tập luật.

Xử lý sự cố

- Ghi lại nhật kí thời gian bị khai thác.
- Ghi lại bộ nhớ của tiến trình tại thời điểm bị xâm nhập, khai thác, hỗ trợ việc điều tra lỗ hổng.

02 NHÓM CHỨC NĂNG CẬP NHẬT

- Nhận lệnh từ server điều khiển tập trung.
- Upload nhật ký về server tập trung khi được server yêu cầu.
- Update RULE từ server tập trung khi được server yêu cầu.
- Upgrade phiên bản mới từ servertập trung khi được server yêu cầu.

03 CÁC HỆ THỐNG TƯƠNG THÍCH

- Base linux.
- CPU: Mips, ARM, X86_64, v.v..

LIÊN HỆ
57 Huỳnh Thúc Kháng – Đống Đa – Hà Nội 0243.7265.171 / 0243.7265.276
https://www.facebook.com/vnptcyberimmunity | sec.vnpt.vn | security@vnpt.vn