**[MTI-13032023/02] Lỗ hổng leo thang đặc quyền trên Microsoft Windows**

**Tóm tắt cảnh báo**

SOC-TI cảnh báo các lỗ hổng mức **Trung Bình** công bố ngày ở sản phẩm Microsoft Windows. Khai thác thành công, tin tặc có thể đạt tới quyền NT AUTHORITY\SYSTEM.

Mã khai thác của lỗ hổng đã được công bố trên không gian mạng.

**Mô tả về lỗ hổng**

* **CVE-2023-21768**: Lỗ hổng leo thang đặc quyền trên hệ điều hành Microsoft Windows

**Phân tích lỗ hổng**

* Lỗ hổng tồn tại trong AFD kernel driver (Ancillary Function Driver). Cụ thể, AFD.sys hiển thị mã điều khiển IO (IO Control Code) "IOCTL\_AFD\_SOCKET\_NOTIFY" cho các tiến trình của người dùng không có đặc quyền, đồng thời cho phép chuyển qua cấu trúc PAFD\_SOCKET\_NOTIFY\_INFO. Trong afd!AfdNotifyRemoveIoCompletion (hàm chịu trách nhiệm cho IOCTL này), nếu lệnh gọi thành công, nó sẽ ghi số lượng entries đã xóa vào trường ReceiveEntryCount - một con trỏ được chỉ định bởi người gọi hàm. Vì hoàn toàn không có xác thực nào được thực hiện ở đây nên tin tặc có thể chuyển một con trỏ tùy ý tới IOCTL và ghi dữ liệu vào, từ đó nâng cao đặc quyền trên hệ thống mục tiêu.
* Tiêu chí khai thác:
  + Tin tặc có thể thực thi mã tùy ý trên máy chủ nhờ khai thác một lỗ hổng khác
* Kết quả khai thác:
  + Tin tặc leo thang đặc quyền lên NT AUTHORITY\SYSTEM.

**Phiên bản bị ảnh hưởng:**

* Windows 11 version 21H2
* Windows 11 Version 22H2
* Windows Server 2022

**Khuyến cáo thực hiện:**

* Quản trị viên kiểm tra các thiết bị có cài đặt phiên bản Windows bị ảnh hưởng
* Thực hiện cập nhật bản vá từ trang chủ Microsoft
* Tham khảo: <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21768>