Investigadores en ciberseguridad han revelado vulnerabilidades en ciertos modelos de cámaras web de Lenovo que podrían transformarlas en dispositivos de ataque tipo BadUSB.

"Esto permite que atacantes remotos inyecten pulsaciones de teclado de forma encubierta y ejecuten ataques independientemente del sistema operativo anfitrión", señalaron en un informe los investigadores de Eclypsium, Paul Asadoorian, Mickey Shkatov y Jesse Michael.

La compañía de seguridad de firmware ha denominado a estas fallas *BadCam*. Los hallazgos fueron presentados hoy durante la conferencia de seguridad DEF CON 33.

Este descubrimiento probablemente marque la primera ocasión en que se demuestra que actores maliciosos que obtienen control de un periférico USB basado en Linux, ya conectado a un equipo, pueden emplearlo con fines maliciosos.

En un escenario hipotético de ataque, un adversario podría aprovechar la vulnerabilidad para enviar a la víctima una cámara web con puerta trasera o conectarla al equipo si logra acceso físico, y posteriormente emitir comandos de manera remota para comprometer el sistema y ejecutar acciones posteriores a la intrusión.

BadUSB, demostrado por primera vez hace más de una década por los investigadores Karsten Nohl y Jakob Lell en la conferencia Black Hat 2014, es un tipo de ataque que explota una vulnerabilidad inherente al firmware USB, reprogramándolo para ejecutar comandos de manera discreta o correr programas maliciosos en la computadora de la víctima.

"A diferencia del malware tradicional, que reside en el sistema de archivos y puede ser detectado por herramientas antivirus, BadUSB se aloja en la capa de firmware", explica Ivanti en una descripción de la amenaza publicada a finales del mes pasado. *"Una vez conectado a un equipo, un dispositivo BadUSB puede: emular un teclado para introducir comandos maliciosos, instalar puertas traseras o registradores de teclas, redirigir el tráfico de internet y extraer información sensible"*.

En años recientes, Mandiant —propiedad de Google— y la Oficina Federal de Investigaciones

(FBI) de EE.UU. han advertido que el grupo de amenazas con motivación financiera identificado como FIN7 ha recurrido al envío de dispositivos USB maliciosos tipo *BadUSB* a organizaciones estadounidenses para distribuir un malware llamado DICELOADER.

Lenovo 510 FHD Webcam

Lenovo Performance FHD Webcam

El hallazgo más reciente de Eclypsium evidencia que un periférico USB, como cámaras web que ejecutan Linux, aun sin ser creado con intención maliciosa, puede convertirse en un vector para ataques BadUSB, representando una escalada notable. Se ha comprobado que estos dispositivos pueden ser secuestrados de forma remota y transformados en dispositivos BadUSB sin necesidad de desconectarlos o sustituirlos físicamente.

"Un atacante que obtenga ejecución remota de código en un sistema puede reescribir el firmware de una cámara web con Linux conectada, reconfigurándola para comportarse como un dispositivo HID malicioso o para emular dispositivos USB adicionales", explicaron los investigadores.

"Una vez armada, la aparentemente inofensiva cámara web puede inyectar pulsaciones de

teclado, entregar cargas maliciosas o servir como punto de persistencia profunda, todo mientras conserva la apariencia y funciones principales de una cámara común".

Además, los actores con capacidad de modificar el firmware de la cámara pueden lograr un mayor nivel de persistencia, permitiéndoles reinfectar el equipo incluso después de que haya sido formateado y el sistema operativo reinstalado.

Las vulnerabilidades encontradas en las cámaras Lenovo 510 FHD y Lenovo Performance FHD están relacionadas con la falta de validación del firmware, lo que las deja expuestas a un compromiso total del software de la cámara mediante ataques tipo BadUSB, dado que ejecutan Linux con soporte para USB Gadget.

Tras la divulgación responsable a Lenovo en abril de 2025, el fabricante de PC lanzó actualizaciones de firmware (versión 4.8.0) para mitigar las fallas y colaboró con la empresa china SigmaStar para desarrollar una herramienta que soluciona el problema.

"Este ataque, único en su tipo, expone un vector sutil pero profundamente problemático: los equipos, tanto empresariales como de consumo, suelen confiar en sus periféricos internos y externos, incluso cuando estos son capaces de ejecutar su propio sistema operativo y aceptar instrucciones remotas", dijo Eclypsium.

"En el caso de las cámaras web con Linux, el firmware sin firmar o con protección deficiente permite que un atacante comprometa no solo el sistema anfitrión, sino también cualquier otro equipo al que se conecte la cámara, propagando la infección y eludiendo los controles tradicionales".