BadCam: bugs de webcam Lenovo baseados em Linux permitem ataques

Data: 2025-08-10 07:34:31

Autor: Inteligência Against Invaders

BadCam: bugs de webcam Lenovo baseados em Linux permitem ataques BadUSB

As falhas da webcam da Lenovo, apelidadas de BadCam, permitem que os invasores as transformem em dispositivos BadUSB para injetar pressionamentos de tecla e lançar ataques independentes do sistema operacional.

Os pesquisadores da Eclypsium encontraram vulnerabilidades em algumas webcams da Lenovo, apelidadas coletivamente de BadCam, que poderiam permitir que invasores as transformassem em BadUSB dispositivos para injetar pressionamentos de tecla e lançar ataques independentes do sistema operacional. Principais pesquisadores de segurança Jesse Michael e Mickey Shkatov demonstrou as falhas na DEF CON 33. Esta é provavelmente a primeira prova de que um periférico USB baseado em Linux comprometido já conectado a um computador pode ser armado para fins maliciosos.

“Os pesquisadores da Eclypsium descobriram que modelos selecionados de webcams da Lenovo executam Linux, não validam o firmware e podem ser armados como dispositivos BadUSB.” lê o relatório publicado pela Eclypsium.

“Até onde sabemos, esta é a primeira vez que foi demonstrado que os invasores podem armar um dispositivo USB que já está conectado a um computador que não foi inicialmente planejado para ser malicioso.”

O BadUSB explora a confiança em dispositivos USB reprogramando o firmware para imitar HIDs e executar comandos maliciosos, ignorando as defesas do sistema operacional. Demonstrado pela primeira vez emBlack Hat 2014 por Karsten Nohl e Jakob Lell em 2014, agora é armado com ferramentas como Patinho de borracha, Nadadeira Zeroe cargas de código aberto. Os ataques são furtivos, modulares e persistentes, muitas vezes evitando a detecção e permitindo roubo de dados, escalonamento de privilégios e ransomware.

Os pesquisadores da Eclypsium demonstraram que periféricos USB baseados em Linux, como webcams, podem ser sequestrados remotamente e convertidos em dispositivos BadUSB sem a necessidade de acesso físico. Ao atualizar o firmware, os invasores podem fazê-los agir como HIDs maliciosos, injetar cargas úteis ou reinfectar hosts persistentemente, mesmo depois que os usuários reinstalam os sistemas operacionais. O recurso de gadget USB do Linux permite que esses dispositivos imitem periféricos confiáveis, ampliando a ameaça a muitos dispositivos USB com Linux.

“Os pesquisadores da Eclypsium, Jesse Michael e Mickey Shaktov, expandiram o cenário de

ameaças do BadUSB, demonstrando que periféricos USB específicos, como webcams rodando Linux, podem ser sequestrados remotamente e transformados em dispositivos BadUSB sem nunca serem fisicamente desconectados ou substituídos. Isso marca uma evolução notável: um invasor que obtém execução remota de código em um sistema pode atualizar novamente o firmware de uma webcam conectada ao Linux, redirecionando-a para se comportar como um HID malicioso ou para emular dispositivos USB adicionais." continua o relatório. "Uma vez armada, a webcam aparentemente inócua pode injetar pressionamentos de tecla, fornecer cargas maliciosas ou servir como um ponto de apoio para uma persistência mais profunda, mantendo a aparência externa e a funcionalidade central de uma câmera padrão."

A Eclypsium descobriu que as webcams Lenovo 510 FHD e Performance FHD são vulneráveis a atualizações de firmware inseguras, permitindo o comprometimento total da câmera. Ambos usam SoCs baseados em SigmaStar ARM rodando Linux com suporte a USB Gadget, permitindo que ataques no estilo BadUSB sequestrem um host. Os pesquisadores descobriram que o processo de atualização carece de salvaguardas, comandos USB simples podem apagar e substituir o flash SPI de 8 MB, permitindo que os invasores substituam o firmware e armem a câmera, mantendo a funcionalidade normal.

Abaixo está um vídeo PoC do ataque:

[VÍDEO/IFRAME REMOVIDO]

A Eclypsium instou a Lenovo e a SigmaStar a adicionar verificação de firmware aos SoCs afetados. A Lenovo respondeu criando uma ferramenta de instalação atualizada com validação de assinatura para corrigir a falha. Os usuários das webcams afetadas devem baixar a atualização do site de suporte da Lenovo para mitigar os riscos. A empresa trabalhou com a SigmaStar para avaliar e resolver a vulnerabilidade prontamente.

"À medida que as cadeias de suprimentos de dispositivos continuam a se diversificar e os periféricos USB se tornam mais complexos, esses ataques ressaltam a necessidade urgente de assinatura de firmware, atestado de dispositivos e visibilidade mais granular do que está conectado aos endpoints corporativos", conclui o relatório. "Com o BadUSB agora possível não apenas por meio de acesso físico, mas também de manipulação remota de periféricos do dia a dia, as organizações devem repensar os modelos de confiança de endpoint e hardware."

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,BadCam)