A Cisco corrige falhas de alta gravidade do IOS XR que permitem desvio d

Data: 2025-09-12 14:51:33

Autor: Inteligência Against Invaders

A Cisco corrige falhas de alta gravidade do IOS XR que permitem desvio de imagem e DoS

A Cisco abordou várias vulnerabilidades de alta gravidade do IOS XR que podem permitir que a verificação de imagem ISO ignore e acione condições de DoS.

A Cisco abordou várias vulnerabilidades no software IOS XR como parte de sua publicação semestral de Software Security Advisory Bundled publicada em 10 de setembro de 2025.

Abaixo estão as vulnerabilidades abordadas pela gigante da rede:

A tabela a seguir identifica o conteúdo do Cisco Security associado a esta publicação agrupada:

A mais grave dessas vulnerabilidades é um problema de alta gravidade, rastreado como CVE-2025-20340, que reside na implementação do Address Resolution Protocol (ARP) do Cisco IOS XR Software. Um invasor adjacente não autenticado pode explorar a falha para acionar uma tempestade de transmissão, acionando uma condição de negação de serviço (DoS) em um dispositivo afetado.

“Essa vulnerabilidade se deve à forma como o Cisco IOS XR Software processa uma taxa alta e sustentada de tráfego ARP que atinge a interface de gerenciamento. Sob certas condições, um invasor pode explorar essa vulnerabilidade enviando uma quantidade excessiva de tráfego para a interface de gerenciamento de um dispositivo afetado, sobrecarregando seus recursos de processamento ARP.” lê o comunicado*. “Uma exploração bem-sucedida pode resultar em desempenho degradado do dispositivo, perda de conectividade de gerenciamento e completa falta de resposta do sistema, levando a uma condição de DoS.”*

Rastreado como CVE-2025-20248 (pontuação CVSS de 6), o primeiro dos bugs é um problema de alta gravidade no processo de instalação do IOS XR que pode permitir que invasores ignorem a verificação de assinatura de imagem.

A exploração bem-sucedida da falha, explica a Cisco, pode levar à adição de arquivos não assinados a uma imagem ISO, que pode ser instalada e ativada em um dispositivo.

Devido ao possível desvio do processo de verificação de imagem, a Cisco elevou a classificação de impacto de segurança do comunicado de médio para alto.

A Cisco corrigiu outro problema de alta gravidade, rastreado como CVE-2025-20248, no processo de

instalação do IOS XR. Invasores com *sistema raiz*no dispositivo afetado podem ignorar verificações de assinatura de imagem, inserir arquivos não assinados em uma imagem ISO e instalá-los em dispositivos.

“Para explorar essa vulnerabilidade, o invasor deve terprivilégios de sistema raiz no dispositivo afetado.” continua o comunicado*. “Esta vulnerabilidade é devido à validação incompleta de arquivos durante a instalação de um arquivo .iso. Um invasor pode explorar essa vulnerabilidade modificando o conteúdo do.isoimage e, em seguida, instalando-o e ativando-o no dispositivo. Uma exploração bem-sucedida pode permitir que o invasor carregue um arquivo não assinado como parte do processo de ativação da imagem.”*

A gigante das redes também corrigiu uma falha IOS XR de gravidade média, rastreada CVE-2025-20159 (CVSS 5.3), que permite que invasores remotos ignorem ACLs para SSH, NetConf e gRPC devido à falta de suporte a ACL na interface de gerenciamento.

A Cisco diz que não tem conhecimento de nenhum ataque em estado selvagem explorando uma dessas vulnerabilidades.

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,IOS XR)