Cisco schließt kritische Sicherheitslücke in seiner Adaptive Security Appliance

Cisco hat eine kritische Sicherheitslücke in seiner Adaptive Security Appliance (ASA) geschlossen. Ein Angreifer kann remote die Kontrolle über eine ASA Appliance übernehmen, die als VPN Server konfiguriert ist. Dafür muss er nur speziell präparierte Netzwerkpakete versenden.

Die Anfälligkeit wird im Common Vulnerability Scoring System (CVSS) mit 10 Punkten bewertet. Das Problem steckt in den Protokollen Internet Key Exchange Version 1 (IKEv1) und IKE Version 2 (IKEv2). Fragmentierte IKE-Pakete können einen Pufferüberlauf auslösen.

Betroffen sind die Cisco ASA 5500 Series Adaptive Security Appliance, Cisco ASA 5500-X Series Next-Generation Firewall, Cisco ASA Services Module für Cisco Catalyst 6500 Series Switches und Cisco 7600 Series Router. Außerdem sind Cisco ASA 1000V Cloud Firewall, Cisco Adaptive Security Virtual Appliance (ASAv), Cisco Firepower 9300 ASA Security Module und Cisco ISA 3000 Industrial Security Appliance anfällig.

„Ein Angreifer kann die Schwachstelle ausnutzen, indem er manipulierte UDP-Pakete an ein betroffenes System verschickt“, schreibt Cisco. „Ein Exploit könnte es einem Angreifer erlauben, Schadcode auszuführen und die vollständige Kontrolle zu übernehmen oder einen Neustart des Systems auszulösen.“

Ich helfe Ihnen gerne diese Lücke zu beseitigen.