ASA 5520 IOS vulnerability of ASA 8.2(1)

A vulnerability in the Secure Sockets Layer (SSL) VPN functionality of the Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to cause a reload of the affected system or to remotely execute code. The vulnerability is due to an attempt to double free a region of memory when the WEBVPN feature is enabled on the Cisco ASA device. An attacker could exploit this vulnerability by sending multiple, crafted XML packets to a WEBVPN-configured interface on the affected system. An exploit could allow the attacker to execute arbitrary code and obtain full control of the system, or cause a reload of the affected device. This vulnerability affects Cisco ASA Software that is running on the following Cisco products: 3000 Series Industrial Security Appliance (ISA), ASA 5500 Series Adaptive Security Appliances, ASA 5500-X Series Next-Generation Firewalls, ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers, ASA 1000V Cloud Firewall, Adaptive Security Virtual Appliance (ASA virtual), Firepower 2100 Series Security Appliance, Firepower 4110 Security Appliance, Firepower 9300 ASA Security Module, Firepower Threat Defense Software (FTD). Cisco Bug IDs: CSCvg35618.