# Multiple Vulnerabilities in Cisco Security Products Could Allow for Arbitra

Data: 2025-08-18 22:31:42

Autor: Inteligência Against Invaders

Multiple vulnerabilities have been discovered in Cisco security products, the most severe of which could allow for arbitrary code execution. Details of the vulnerabilities are as follows:

**Tactic**: *Initial Access* (TA0001):

**Technique**: *Exploit Public-Facing Application* (T1190):

- A vulnerability in the RADIUS subsystem implementation of Cisco Secure Firewall Management Center (FMC) Software could allow an unauthenticated, remote attacker to inject arbitrary shell commands that are executed by the device. (CVE-2025-20265)

Additional lower severity vulnerabilities include:

- A vulnerability in the packet inspection functionality of the Snort 3 Detection Engine of Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. (CVE-2025-20217)
- A vulnerability in the RADIUS proxy feature for the IPsec VPN feature of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS). (CVE-2025-20222)
- A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software could allow an authenticated, remote attacker to inject arbitrary HTML content into a device-generated document. (CVE-2025-20148)
- A vulnerability in the Remote Access SSL VPN service for Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow a remote attacker that is authenticated as a VPN user to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. (CVE-2025-20244)
- Multiple vulnerabilities in the management and VPN web servers for Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to stop responding or reload unexpectedly, resulting in a denial of service (DoS) condition. (CVE-2025-20243, CVE-2025-20133)
- A vulnerability in the certificate processing of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. (CVE-2025-20134)
- A vulnerability in the function that performs IPv4 and IPv6 Network Address Translation (NAT) DNS inspection for Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and

Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. (CVE-2025-20136)

- A vulnerability in the Remote Access SSL VPN service for Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an authenticated, remote attacker to create or delete arbitrary files on the underlying operating system. If critical system files are manipulated, new Remote Access SSL VPN sessions could be denied and existing sessions could be dropped, causing a denial of service (DoS) condition. An exploited device requires a manual reboot to recover. (CVE-2025-20251)
- Multiple vulnerabilities in the Internet Key Exchange Version 2 (IKEv2) feature of Cisco IOS Software, Cisco IOS XE Software, Cisco Secure Firewall Adaptive Security Appliance (ASA) Software, and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. (CVE-2025-20224, CVE-2025-20225, CVE-2025-20239, CVE-2025-20252, CVE-2025-20253, CVE-2025-20254)
- A vulnerability in the web services interface of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a buffer overflow on an affected system. (CVE-2025-20263)
- A vulnerability in the TLS 1.3 implementation for a specific cipher for Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software for Cisco Firepower 3100 and 4200 Series devices could allow an authenticated, remote attacker to consume resources that are associated with incoming TLS 1.3 connections, which eventually could cause the device to stop accepting any new SSL/TLS or VPN requests. (CVE-2025-20127)
- A vulnerability in the Geolocation-Based Remote Access (RA) VPN feature of Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass configured policies to allow or deny HTTP connections based on a country or region. (CVE-2025-20268)
- A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. (CVE-2025-20235)
- A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software could allow an authenticated, remote attacker to retrieve sensitive information from an affected device. (CVE-2025-20218)
- A vulnerability in the CLI of Cisco Secure Firewall Management Center (FMC) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system as root.(CVE-2025-20220)
- A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software could allow an authenticated, remote attacker with Administrator-level privileges to execute arbitrary commands on the underlying operating system. (CVE-2025-20306)
- Multiple vulnerabilities in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software could allow an authenticated, remote attacker to access files that they are not authorized to access.(CVE-2025-20301, CVE-2025-20302)
- A vulnerability in the DHCP client functionality of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, adjacent attacker to exhaust available memory. (CVE-2025-20135)

- Multiple vulnerabilities in Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. To exploit these vulnerabilities, the attacker must have valid administrative credentials. (CVE-2025-20237, CVE-2025-20238)
- A vulnerability in the implementation of access control rules for loopback interfaces in Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to send traffic that should have been blocked to a loopback interface. (CVE-2025-20219)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the user associated with the service.Depending on the privileges associated with the account, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.