Multiple Vulnerabilities in Cisco Products Could Allow for Remote Code Ex

Data: 2025-09-27 00:12:42

Autor: Inteligência Against Invaders

MS-ISAC ADVISORY NUMBER:

2025-091

DATE(S) ISSUED:

09/25/2025

OVERVIEW:

Multiple vulnerabilities have been discovered in Cisco products, the most severe of which could allow for remote code execution. Cisco is a leading technology company best known for its networking hardware and software, such as routers and switches, that form the backbone of the internet and enterprise networks. Successful exploitation of the most severe of these vulnerabilitiescould allow for remote code execution as root, which may lead to the complete compromise of the affected device.

THREAT INTELLIGENCE:

The Cisco Product Security Incident Response Team (PSIRT) is aware of attempted exploitation of CVE-2025-20333 and CVE-2025-20362. A detection guide can be found in the references section further down this advisory.

SYSTEMS AFFECTED:

- Cisco Secure Firewall ASA Software
- Cisco Secure FTD Software
- Cisco Secure FMC Software
- Cisco IOS and IOS XE Software
- Cisco IOS XR Software

RISK:

Government:

Large and medium government entitiesHIGH

Small governmentMEDIUM

Businesses:

Large and medium business entitiesHIGH

Small business entitiesMEDIUM

TECHNICAL SUMMARY:

Tactic: *Initial Access* (TA0001):

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

- A vulnerability in the VPN web server of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to access restricted URL endpoints without authentication that should otherwise be inaccessible without authentication. This vulnerability is due to

improper validation of user-supplied input in HTTP(S) requests. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted web server on a device. A successful exploit could allow the attacker to access a restricted URL without authentication. (CVE-2025-20362)

- A vulnerability in the VPN web server of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an authenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to improper validation of user-supplied input in HTTP(S) requests. An attacker with valid VPN user credentials could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as root, possibly resulting in the complete compromise of the affected device. (CVE-2025-20333)
- A vulnerability in the web services of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software, Cisco Secure Firewall Threat Defense (FTD) Software, Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software could allow an unauthenticated, remote attacker (Cisco ASA and FTD Software) or authenticated, remote attacker (Cisco IOS, IOS XE, and IOS XR Software) with low user privileges to execute arbitrary code on an affected device. This vulnerability is due to improper validation of user-supplied input in HTTP requests. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted web service on an affected device after obtaining additional information about the system, overcoming exploit mitigations, or both. A successful exploit could allow the attacker to execute arbitrary code as root, which may lead to the complete compromise of the affected device. (CVE-2025-20363)

Successful exploitation of the most severe of these vulnerabilitiescould allow for remote code execution as root, which may lead to the complete compromise of the affected device.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate updates provided by Cisco or other vendors which use this software to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)
- **Safeguard 7.1 : Establish and Maintain a Vulnerability Management Process:** Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
- **Safeguard 7.2: Establish and Maintain a Remediation Process:**Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
- **Safeguard 7.4: Perform Automated Application Patch Management:**Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
- **Safeguard 7.5 : Perform Automated Vulnerability Scans of Internal Enterprise**

Assets: Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.

- **Safeguard 7.7: Remediate Detected Vulnerabilities:**Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
- **Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date:**Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.
- **Safeguard 18.1: Establish and Maintain a Penetration Testing Program:**Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
- **Safeguard 18.2: Perform Periodic External Penetration Tests:**Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.
- **Safeguard 18.3: Remediate Penetration Test Findings:**Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.

- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)
- **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:**Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
- **Safeguard 5.5: Establish and Maintain an Inventory of Service Accounts:**Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

- Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them. (**M1016**:**Vulnerability Scanning**)
- **Safeguard 16.13: Conduct Application Penetration Testing:**Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.

- Architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network. Configure separate virtual private cloud (VPC) instances to isolate

critical cloud systems. (M1030:**Network Segmentation**)

- **Safeguard 12.2: Establish and Maintain a Secure Network Architecture:** Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.

- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (M1050:**Exploit Protection**)
- **Safeguard 10.5:Enable Anti-Exploitation Features:**Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.