Cisco Addresses Cisco Catalyst Center Arbitrary File Read Vulnerability

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

Cisco has released security updates for a high-severity arbitrary file read vulnerability (CVE-2026-20191, CVSS 7.5) affecting Cisco Catalyst Center and Cisco Catalyst Center Global Manager.

The vulnerability may allow an unauthenticated remote attacker to read sensitive files from affected systems, potentially exposing information that could be used to launch additional attacks.

Overview

There is a high-severity vulnerability (CVE-2026-20191, CVSS 7.5) in Cisco Catalyst Center and Cisco Catalyst Center Global Manager.

Cisco Catalyst Center is a centralized management platform for Cisco enterprise networks. IT teams use it to manage Cisco network devices and monitor enterprise networks from a central console.

Affected Products

- Cisco Catalyst Center hardware appliances
- Cisco Catalyst Center Virtual Appliances on AWS
- Cisco Catalyst Center Virtual Appliances on Microsoft Azure
- Cisco Catalyst Center Virtual Appliances on VMware ESXi
- Cisco Catalyst Center Global Manager

CVE-2026-20191 is caused by insufficient validation of user-supplied input. An unauthenticated attacker can send a crafted HTTP request to read arbitrary files from a restricted container on an affected device. Successful exploitation may expose sensitive configuration files or other information that could assist an attacker in launching additional attacks.

While this vulnerability does not directly impact firewalls, a compromised Catalyst Center server could expose sensitive network information that may assist attackers targeting the enterprise. The vulnerability has not been exploited at this time. Aspire recommends applying the available security updates as soon as possible.

Aspire Protects

- **Patch** – Upgrade affected Cisco Catalyst Center and Cisco Catalyst Center Global Manager deployments to the appropriate fixed software release.
- Identify all Cisco Catalyst Center deployments within the environment.
- Restrict access to Catalyst Center management interfaces to trusted administrative networks.
- Review logs for suspicious HTTP requests targeting Catalyst Center.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – Threat actors may exploit an internet-facing Cisco Catalyst Center management interface to read sensitive files.

Discovery

- File and Directory Discovery [T1083] – Threat actors may enumerate accessible files and directories after successfully exploiting the vulnerability.

Collection

- Data from Local System [T1005] – Threat actors may collect sensitive configuration files or other locally stored information from the affected appliance.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Organizations using Cisco Catalyst Center to centrally manage enterprise network infrastructure may be affected, especially those in:

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Cisco Catalyst Center Arbitrary File Read Vulnerability