




Malware & Threats ▾ Security Operations ▾ Security Architecture ▾

Risk Management ▾ CISO Strategy ▾ ICS/OT ▾ Funding/M&A ▾

DEVO

Journey to the Autonomous SOC

[Download Now](#)



aws Available in AWS Marketplace

VULNERABILITIES

Cisco Patches High-Severity Vulnerabilities in ACI Components

Cisco has patched DoS and CSRF vulnerabilities in the Application Policy Infrastructure Controller (APIC) and Nexus 9000 series switches.



By [Eduard Kovacs](#)
February 23, 2023



Cisco on Wednesday informed customers about the availability of patches for two high-severity vulnerabilities affecting components of its Application Centric Infrastructure (ACI)

TRENDING

- 1 AI Helps Crack NIST-Recommended Post-Quantum Encryption Algorithm
- 2 Apple Updates Advisories as Security Firm Discloses New Class of Vulnerabilities
- 3 VMware Plugs Critical Carbon Black App Control Flaw

software-defined networking solution.

One of these flaws, CVE-2023-20011, impacts the management interface of the Cisco Application Policy Infrastructure Controller (APIC) and Cloud Network Controller. APIC is the unified point of automation and management for ACI.

The vulnerability can be exploited by a remote, unauthenticated attacker to conduct cross-site request forgery (CSRF) attacks by tricking a user into clicking on a malicious link. The attacker could then conduct activities on the targeted system with the privileges of the compromised user.

The second high-severity issue, CVE-2023-20089, affects Cisco Nexus 9000 series Fabric switches in ACI mode, and it can be exploited for denial-of-service (DoS) attacks by an unauthenticated, adjacent attacker. The vendor noted that certain conditions need to be met for exploitation.

Both security holes were discovered internally and there is no evidence of malicious exploitation.

- 4** **Stealthy Mac Malware Delivered via Pirated Apps**
- 5** **CISA Warns of Two Mitel Vulnerabilities Exploited in Wild**
- 6** **R1Soft Server Backup Manager Vulnerability Exploited to Deploy Backdoor**
- 7** **Cisco Patches High-Severity Vulnerabilities in ACI Components**
- 8** **SolarWinds Announces Upcoming Patches for High-Severity Vulnerabilities**

Daily Briefing Newsletter

Subscribe to the SecurityWeek Email Briefing to stay informed on the latest

In addition, Cisco has patched medium-severity flaws in several products, including a UCS Manager and FXOS software issue that exposes backup files, a command injection bug in NX-OS, a command injection in Firepower appliances, and an authentication bypass vulnerability in Nexus extenders (requires physical access).

The networking giant has also released an informational advisory for a privilege escalation issue related to products running NX-OS software and configured for SSH authentication with an X.509v3 certificate.

Cisco on Wednesday also updated its advisory for CVE-2023-20032, a recently addressed [critical vulnerability affecting the ClamAV library](#). The company has informed customers about the availability of technical information describing CVE-2023-20032, and the existence of a proof-of-concept (PoC) exploit. There is currently no evidence of malicious exploitation.

Additional information can be found in [Cisco's security advisories](#).

threats, trends, and technology, along with insightful columns from industry experts.

Webinar: Building Sustainable OT Cybersecurity Programs

🕒 Thursday, February 23, 2023

Join this webinar to gain clear advice on the people, process and technology considerations that must be made at every stage of an OT security program's lifecycle.

[Register](#)

Webinar: Entering the Cloud Native Security Era

🕒 Thursday, March 02, 2023

This presentation will provide an overview of the security risks associated with SaaS, best practices for mitigating these risks and protecting data, and discuss the importance of regularly reviewing and updating SaaS security practices to ensure ongoing protection of data.

[Register](#)

EXPERT INSIGHTS

Enterprise Blind Spots and Obsolete Tools – Security Teams Must Evolve



The conventional tools we rely on to defend corporate networks are creating gaps in network visibility and in our capabilities to secure them.

[\(Matt Wilson\)](#)