MITRE Caldera security advisory warns of maximum severity flaw





A security advisory has been issued for MITRE Caldera, warning of a a Remote Code Execution (RCE) vulnerability. This vulnerability (CVE-2025-27364) was discovered in the server's dynamic compilation functionality, specifically the Manx and Sandcat agents (implants). Malicious actors could exploit this flaw to execute arbitrary code on servers Caldera is running on.

Security leaders weigh in

Thomas Richards, Principal Consultant, Network and Red Team Practice Director at Black Duck:

Caldera is one of the primary tools used by an organization's internal red team to perform continuous and automated testing against their organization. It quickly became the standard since it was open source and supported by a major cyber security organization. Tools like this often have elevated privilege and access to other systems for them to perform the work properly. If Caldera or any organization-wide security tool gets compromised, it would put the attacker in a position to compromise additional systems throughout the organization. Software risk is a business risk and given the prevalence of this tool, organizations should take steps to immediately patch the software and investigate if there were any breaches.

Mr. Mayuresh Dani, Manager, Security Research, at Qualys Threat Research Unit:

CVE-2025-27364 is a critical vulnerability in one of most popular and open source, autonomous adversary emulation frameworks – MITRE Caldera. The remote code execution vulnerability exists because of insufficient imposition of security restrictions and input sanitization in Caldera's agent compilation process. This vulnerability affects the Caldera Manx and Sandcat agents that call back to the server, when Go, python and gcc are installed on the system that the Caldera server is running on. Successful exploitation allows a remote, unauthenticated threat actor to execute arbitrary code on the server running Caldera, leading to a complete system compromise.

MITRE Caldera is used by both – security defenders to automate testing of cyber defenses and offensive security teams to augment their testing efforts. Since MITRE Caldera is an open source emulation framework and is compatible across Linux, Apple Mac OS, Microsoft Windows (implants) operating systems, the use is widespread. The vulnerability exists in the implant compilation endpoint, and can be trivially triggered by an unauthenticated threat actor using a simple curl command. Though the proof-of-concept code is not weaponized and needs a slight modification, it can be easily discovered.

I have seen organizations modify implants for their needs, but the server API is normally untouched, warranting updates to the latest version. Furthermore, since its use in an organization is known and sanctioned, exploitation of the MITRE Caldera server can potentially go unsupervised. Once the server is compromised the attacker could gain access to all the implants and launch further attacks inside the network. This can turn out to be a perfect playing ground for a threat actor.

Eric Schwake, Director of Cybersecurity Strategy at Salt Security:

The vulnerability found in the MITRE Caldera platform poses a significant risk for organizations that depend on it for adversary emulation and security testing. Its security is paramount as a widely utilized tool among security researchers, red teams, and professionals involved in threat modeling and vulnerability assessment. The ability of a remote attacker to execute arbitrary code on the Caldera server, mainly via its API, raises serious concerns.

In a worst-case scenario, an attacker could gain full control of the server, potentially compromising sensitive data, skewing test results, or even utilizing the platform for further attacks on other systems within the organization. This scenario underscores the urgent need for immediate patching of this vulnerability. Organizations using Caldera must prioritize upgrading to the latest version and implementing any additional security measures recommended by MITRE.

This situation also serves as a wider reminder of the necessity for strong API security practices. The existence of this vulnerability within the Caldera server API highlights how APIs can become attractive targets for attackers. Adopting robust API security measures, including thorough authentication, authorization, input validation, and consistent security testing, is essential to prevent such breaches. A holistic approach to API posture governance can aid organizations in identifying and mitigating API vulnerabilities, ensuring that APIs are securely configured and in line with industry standards. While this specific flaw is within the Caldera platform, the principle of securing APIs is universal across all organizations and systems.

https://www.securitymagazine.com/articles/101428-mitre-caldera-security-advisory-warns-of-maximum-severity-flaw