NVD DB Update

CVE-2025-27364 - Score: 10.0

Components:

Description:

In MITRE Caldera through 4.2.0 and 5.0.0 before 35bc06e, a Remote Code Execution (RCE) vulnerability was found in the dynamic agent (implant) compilation functionality of the server. This allows remote attackers to execute arbitrary code on the server that Caldera is running on via a crafted web request to the Caldera server API used for compiling and downloading of Caldera's Sandcat or Manx agent (implants). This web request can use the gcc -extldflags linker flag with sub-commands.

Main problems:

78 "Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')"

https://cybersword.tech
ph1sher

www.linkedin.com/in/cybersword-tech
@davidwowa