NVD DB Update

CVE-2025-1040 - Score: 8.8

Components:

agpt autogpt *

Description:

AutoGPT versions 0.3.4 and earlier are vulnerable to a Server-Side Template Injection (SSTI) that could lead to Remote Code Execution (RCE). The vulnerability arises from the improper handling of user-supplied format strings in the ‘ AgentOutputBlock‘ implementation, where malicious input is passed to the Jinja2 templating engine without adequate security measures. Attackers can exploit this flaw to execute arbitrary commands on the host system. The issue is fixed in version 0.4.0.

Main problems:

77 no CWE Description available