NVD DB Update

CVE-2024-40629 - Score: 10.0

Components:

fit2cloud jumpserver *

Description:

JumpServer is an open-source Privileged Access Management (PAM) tool that provides DevOps and IT teams with on-demand and secure access to SSH, RDP, Kubernetes, Database and RemoteApp endpoints through a web browser. An attacker can exploit the Ansible playbook to write arbitrary files, leading to remote code execution (RCE) in the Celery container. The Celery container runs as root and has database access, allowing an attacker to steal all secrets for hosts, create a new JumpServer account with admin privileges, or manipulate the database in other ways. This issue has been patched in release versions 3.10.12 and 4.0.0. It is recommended to upgrade the safe versions. There are no known workarounds for this vulnerability.

Main problems:

22 "Improper Limitation of a Pathname to a Restricted Directory (’Path Traversal’)"