CVE-2023-52138 - Score: 8.2

Components:

mate-desktop engrampa *

Description:

Engrampa is an archive manager for the MATE environment. Engrampa is found to be vulnerable to a Path Traversal vulnerability that can be leveraged to achieve full Remote Command Execution (RCE) on the target. While handling CPIO archives, the Engrampa Archive manager follows symlink, cpio by default will follow stored symlinks while extracting and the Archiver will not check the symlink location, which leads to arbitrary file writes to unintended locations. When the victim extracts the archive, the attacker can craft a malicious cpio or ISO archive to achieve RCE on the target system. This vulnerability was fixed in commit 63d5dfa.

Main problems:

25 no CWE Description available