CVE-2024-25626 - Score: 8.8

Components:

linuxfoundation yocto *

Description:

Yocto Project is an open source collaboration project that helps developers create custom Linux-based systems regardless of the hardware architecture. In Yocto Projects Bitbake before 2.6.2 (before and included Yocto Project 4.3.1), with the Toaster server (included in bitbake) running, missing input validation allows an attacker to perform a remote code execution in the server's shell via a crafted HTTP request. Authentication is not necessary. Toaster server execution has to be specifically run and is not the default for Bitbake command line builds, it is only used for the Toaster web based user interface to Bitbake. The fix has been backported to the bitbake included with Yocto Project 5.0, 3.1.31, 4.0.16, and 4.3.2.

Main problems:

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