

microsoft binwalk \*

### Description:

A path traversal vulnerability was identified in ReFirm Labs binwalk from version 2.1.2b through 2.3.3 included. By crafting a malicious PFS filesystem file, an attacker can get binwalk's PFS extractor to extract files at arbitrary locations when binwalk is run in extraction mode (-e option). Remote code execution can be achieved by building a PFS filesystem that, upon extraction, would extract a malicious binwalk module into the folder .config/binwalk/plugins. This vulnerability is associated with program files src/binwalk/plugins/unpfs.py. This issue affects binwalk from 2.1.2b through 2.3.3 included.

### Main problems:

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