NVD DB Update

CVE-2025-0678 - Score: 6.4

Components:

gnu grub2 *

Description:

A flaw was found in grub2. When reading data from a squash4 filesystem, grub's squash4 fs module uses user-controlled parameters from the filesystem geometry to determine the internal buffer size, however, it improperly checks for integer overflows. A maliciously crafted filesystem may lead some of those buffer size calculations to overflow, causing it to perform a grub_malloc() operation with a smaller size than expected. As a result, the direct_read() will perform a heap based out-of-bounds write during data reading. This flaw may be leveraged to corrupt grub's internal critical data and may result in arbitrary code execution, by-passing secure boot protections.

Main problems:

190 "Integer Overflow or Wraparound"

https://cybersword.tech
ph1sher

www.linkedin.com/in/cybersword-tech
@davidwowa