NVD DB Update

CVE-2025-0677 - Score: 6.4

Components:

Description:

A flaw was found in grub2. When performing a symlink lookup, the grub’s UFS module checks the inode’s data size to allocate the internal buffer to read the file content, however, it fails to check if the symlink data size has overflown. When this occurs, grub_malloc() may be called with a smaller value than needed. When further reading the data from the disk into the buffer, the grub_ufs_lookup_symlink() function will write past the end of the allocated size. An attack can leverage this by crafting a malicious filesystem, and as a result, it will corrupt data stored in the heap, allowing for arbitrary code execution used to by-pass secure boot mechanisms.

Main problems:

787 "Out-of-bounds Write"