Immunity, Inc. Advisory

Disclosure

This advisory has been released and may be redistributed in full. Other use is prohibited.

Vulnerability

Local root exploit against Solaris.

A directory traversal problem exists in vfs_getvfssw() in the Solaris kernel which allows an attacker to load a user-specified kernel module.

The bug is exploitable via either the mount() or sysfs() system calls.

Affected

Solaris 2.6 through 10 are affected by this vulnerability.

Detection

Immunity Research has provided a working exploit for this problem. (See o0o0.tgz)

For questions or comments, please contact Immunity, Inc. at dave@immunitysec.com, or http://www.immunitysec.com.

History

Found by Immunity Researcher Sinan Eren, December, 2003.