SUID/SGID Scripts

Category: Security Policies

Users are prohibited from creating and using privileged SUID and/or SGID scripts under their home, scratch, **`/nobackup`**, and **`/tmp`** filesystems.

SUID scripts (that is, with permission **`u+s`**) and SGID scripts (with permission **`g+s`**) could allow someone (other than the owner) to gain unauthorized access to users' files, posing a security hazard.

WARNING: The high end computing systems at the NAS facility are configured to disable the execution of any SUID/SGID shell scripts.

Article ID: 263
Last updated: 08 Aug, 2012
Policies -> Security Policies -> SUID/SGID Scripts
http://www.nas.nasa.gov/hecc/support/kb/entry/263/?ajax=1