

Bad bug in SUS utility allows users to gain root access

LinuxReviews.org

SUS is a small tool that, like SuDO, allows regular users on a system to execute given allowed commands as root. A bug in SUS < 2.0.2 actually allows any user on a system with SUS to run ANY command as root.

This only affects systems where SUS is installed. Sudo, a similar utility, is much more commonly used for this purpose, and is known to be perfectly safe.

System administrators who use SUS should immediately upgrade to the latest available version. Leon Juranic from LSS Security found a format string vulnerability in the logging functionality due to an incorrect call to the function syslog().

This can, in a worst case scenario, allow a skilled local user to run any command as root. The user must already have a valid user account on the targeted system.

From the change-log: 2.0.6 - Sept 14, 2004 Fixed a security problem in call to syslog in log.c. All users should upgrade to 2.0.6 as soon as possible. Many thanks to Leon Juranic from LSS Security (<http://security.lss.hr>) for finding this problem...

- SUS ChangeLog (pdg.uow.edu.au)
- BugTraq Advisory (securityfocus.com)
- GLSA 200409-17 / SUS (gentoo.org)
- eXposed by LSS

> [Linux Reviews](#) > [News and headlines](#) > [2004 News archive](#) > [September](#)
>
Bad bug in SUS utility allows users to gain root access