

# EXAScaler™

## Security Issue with Files Created in Linux SGID Directories

---

**ALERT!** A Linux kernel bug allows local users to create files with unintended group ownership in SGID directories. An attacker could exploit this bug to escalate privileges and make a plain file executable with group permissions.

---

### Issue Summary

Linux provides certain permission management features that simplify file sharing. The “set user identification” (SUID) feature can be enabled only on files. When enabled on an executable file, that executable runs with the permissions of the creator of the file, not those of the user executing it. The “set group identification” (SGID) feature is similar, and can be enabled on both files and directories. When SGID is enabled on an executable file, the file runs with the permissions of the group to which the file belongs, not those of the file creator or the user executing it. When SGID is enabled on a directory, new files created in that directory inherit the permissions of the group that owns the directory, not those of the file creator.

A Linux kernel bug allows local users to create files with unintended group ownership in SGID directories. An attacker who is not a group member could exploit this bug to escalate privileges and make a plain file executable with group permissions.

This bug is identified as [CVE-2018-13405](#) in the National Vulnerability Database maintained by the National Institute for Standards and Technology (NIST).

## Affected Products

Linux kernel versions through 4.17.4 are affected by the SGID bug. Affected kernel versions are bundled with EXAScaler versions 4.1.x and earlier. EXAScaler 4.2 incorporates the kernel fix for this issue and is **not** affected by the SGID bug.

## Resolution

To resolve this issue, DDN recommends that customers upgrade to EXAScaler 4.2 or higher as soon as possible. Please contact DDN Support to obtain an upgrade plan and installation assistance.

## Workaround

To mitigate this issue until a maintenance window for upgrade becomes available, DDN recommends that all clients mount Lustre with the following mount option:

```
-o nosuid
```

## Contacting DDN Technical Support

Please contact DDN Technical Support at any time if you have questions or require assistance. Support can be reached by phone, by email, or on the web as listed below.

### Web

*DDN Community Support Portal*  
*Portal Assistance*

<https://community.ddn.com/login>  
[webportal.support@ddn.com](mailto:webportal.support@ddn.com)

### Telephone

*DDN Support Worldwide Directory*

<https://www.ddn.com/support/global-services-overview/>

### Email

*Support Email*

[support@ddn.com](mailto:support@ddn.com)

### Bulletins

*Support Bulletins*  
*End-of-Life Notices*  
*Bulletin Subscription Requests*

<http://www.ddn.com/support/technical-support-bulletins>  
<http://www.ddn.com/support/end-of-life-notices>  
[support-tsb@ddn.com](mailto:support-tsb@ddn.com)