CERT Advisory CA-1997-15 Vulnerability in SGI login LOCKOUT

Original issue date: May 28, 1997
Last revised: September 30, 1997
Updated copyright statement

A complete revision history is at the end of this file.

The text of this advisory was originally released on April 10, 1997, as AUSCERT Advisory AA-97.12, developed by the Australian Computer Emergency Response Team. To more widely broadcast this information, we are reprinting the AUSCERT advisory here with their permission. Only the contact information at the end has changed: AUSCERT contact information has been replaced with CERT/CC contact information.

We will update this advisory as we receive additional information. Look for it in an "Updates" section at the end of the advisory.

AUSCERT has received information that a vulnerability exists in the login program when the LOCKOUT parameter in /etc/default/login is set to a number greater than zero. This vulnerability is known to be present in IRIX 5.3 and 6.2. Other versions of IRIX may also be vulnerable.

This vulnerability may allow users to create arbitrary or corrupt certain files on the system.

Exploit information involving this vulnerability has been made publicly available.

At this stage, AUSCERT is unaware of any official vendor patches. AUSCERT recommends that sites apply the workaround given in Section 3 until vendor patches are made available.

This advisory will be updated as more information becomes available.

---

1. Description

Under the IRIX operating system, there is a file /etc/default/login which contains default security logging configuration options. If the parameter LOCKOUT is included in this file, and is set to a value greater than zero, it causes accounts to be locked after a specified number of consecutive unsuccessful login attempts by the same user.

When LOCKOUT is enabled users may be able to create arbitrary or corrupt certain files on the system, due to an inadequate check in the login verification process.

Sites can determine if this functionality is enabled by using the command:

```
% grep '^LOCKOUT' /etc/default/login
LOCKOUT=3
```

If the number on the same line as LOCKOUT is greater than zero the vulnerability may be exploited.
Information involving this vulnerability has been made publicly available.

Silicon Graphics Inc. has informed AUSCERT that they are investigating this vulnerability.

2. Impact

Users may create arbitrary or corrupt certain files on the system.

3. Workarounds/Solution

AUSCERT recommends that sites prevent the exploitation of this vulnerability by immediately applying the workaround given in Section 3.1.

Currently there are no vendor patches available that address this vulnerability. AUSCERT recommends that official vendor patches be installed when they are made available.

3.1 Disable the LOCKOUT parameter

To prevent the exploitation of the vulnerability described in this advisory, AUSCERT recommends that the functionality provided with the LOCKOUT parameter be disabled.

The LOCKOUT parameter can be disabled by editing /etc/default/login and commenting out the line containing the LOCKOUT parameter. The comment character for /etc/default/login is "#".

Note that after applying this workaround, accounts will not be automatically locked using the LOCKOUT parameter functionality.

AUSCERT thanks to Alan J Rosenthal from The University of Toronto and Silicon Graphics Inc. for their assistance in this matter.

UPDATES

May 28, 1997

After the AUSCERT advisory was published, we received this information from Silicon Graphics:

At this time, Silicon Graphics does not have any public information for the login LOCKOUT issue. Silicon Graphics has communicated with CERT/CC and other external security parties and is actively investigating this issue. When more Silicon Graphics information (including any possible patches) is availavble for release, that information will be released via the SGI security mailing list, wiretap.

For subscribing to the wiretap mailing list and other SGI security related information, please refer to the Silicon Graphics Security Headquarters website at:

http://www.sgi.com/Support/Secur/security.html

Revision History

```
Sept. 30, 1997 Updated copyright statement
Sept. 19, 1997 Updates Section. Added updated vendor information for
 Silicon Graphics, Inc.
```