

[UNIX] Openwebmail Remote Root Compromise

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-12/0093.html>

From: support@securiteam.com

Date: 12/26/02

From: support@securiteam.com

To: list@securiteam.com

Date: 26 Dec 2002 23:26:00 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Openwebmail Remote Root Compromise

SUMMARY

<<http://openwebmail.org/>> Openwebmail is a web-based email system. It contains several Perl CGI scripts run under superuser account (suidperl is used). A remote exploitation of several errors within the Openwebmail scripts could allow a remote attacker to execute arbitrary commands with the superuser permissions. Although this requires attacker to be able to put 2 files on target system (i.e. via FTP or if he has local shell access), this is a very serious vulnerability and should be taken seriously.

DETAILS

Vulnerable systems:

* Openwebmail version 1.71 and prior

If we inspect the sources:

---- openwebmail-abook.pl

#!/usr/bin/suidperl -T

..

require "openwebmail-shared.pl";

..

openwebmail_init();

Securiteam: [UNIX] Openwebmail Remote Root Compromise

```
..
- ----
- ---- openwebmail-shared.pl
..
sub openwebmail_init {
..
  $thissession = param("sessionid"); # (0)
..
  $loginname =~ s/\-session\-0.*$//; # (1)

  my $siteconf;
  if ($loginname =~ /\^(.+)$/) {
    $siteconf = "$config{'ow_etcdir'}/sites.conf/$1"; # (2)
  } else {
    my $httphost = $ENV{'HTTP_HOST'}; $httphost =~ s/:\d+$//;
    $siteconf = "$config{'ow_etcdir'}/sites.conf/$httphost";
  }
  readconf(\%config, \%config_raw, "$siteconf") if ( -f "$siteconf" ); #
(3)
..
  require $config{'auth_module'}; # (4)
- ----
```

(0) Attacker can pass anything here:

[http://site.url/cgi-bin/openwebmail-abook.pl?sessionid=@\[PATH\]-session-0](http://site.url/cgi-bin/openwebmail-abook.pl?sessionid=@[PATH]-session-0)

(1) \$loginname now holds [PATH] (i.e. `"../../../../../../home/ftp/incoming/attacker.conf"`)

(2) \$siteconf holds path to custom config file on the server. Attacker can upload config file via anonymous ftp (is any), or just put it somewhere (if he has local access)

(3) readconfig() treats \$siteconf as a plaintext file every string of which has format:

```
- ---
var_name variable_value
- ---
```

In our case, <attacker.conf> should contain line

```
- ---
auth_module /home/ftp/incoming/exploit.pl
- ---
```

(4) <exploit.pl> is executed with superuser permissions.

Detection:

To detect whether or not you are running a vulnerable version of the openwebmail software or not, check the responses of cgi scripts. For example:

Securiteam: [UNIX] Openwebmail Remote Root Compromise

```
[user@host][~]: lynx -dump http://site/cgi-bin/openwebmail/openwebmail.pl
| grep -i "version"
      Open WebMail version 1.71
```

Recommendations:

Temporary disable using of openwebmail until patch will be released by the vendor or fix openwebmail-shared.pl, changing:

```
$loginname =~ s/\-session\-0.*$/; # Grab loginname from sessionid
```

Into

```
$loginname =~ s/\-session\-0.*$/; # Grab loginname from sessionid
```

```
$loginname =~ s/[\\|;|\\|\"\\|&|/|g;
```

```
$loginname =~ s/\\.//g;
```

Patch:

A patch is available from the following web site:

<<http://openwebmail.org/openwebmail/download/cert/patches/SA-02:01/>>
<http://openwebmail.org/openwebmail/download/cert/patches/SA-02:01/>

ADDITIONAL INFORMATION

The information has been provided by <mailto:demiurg@altaee.com> Dmitry Guyvoronsky and <mailto:Stephan.Sachweh@pallas.com> Stephan Sachweh.

=====

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.