

[UNIX] IMP Allows Arbitrary File Reading and Path Disclosure

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0073.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/23/03

To: list@securiteam.com

Date: 23 Jun 2003 10:56:21 +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 in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

IMP Allows Arbitrary File Reading and Path Disclosure

SUMMARY

<<http://www.horde.org>> IMP (Internet Messaging Program) is a popular application, written in PHP which provides WebMail access to any IMAP or POP3 mailbox, and handles Internet standard MIME attachments, user defined filters, preferences, and more. A vulnerability in the product allows both arbitrary file reading and path disclosure vulnerabilities.

DETAILS

Elia Florio has found a security bug in the CSS manipulation page ([index.php](#)) of IMP, inside the admin section of the web-interface. If an user uses this page:

<http://www.somesite.com/horde/admin/css/index.php>

He can select the best CSS (cascade style-sheet) for IMP pages, using a special StyleSheet Editor, written in PHP. In the standard installation of IMP there are some CSS files showed in a ListBox of the page "index.php".

Securiteam: [UNIX] IMP Allows Arbitrary File Reading and Path Disclosure

```
../../config/html.php  
../../imp/config/html.php  
../../turba/config/html.php
```

Selection of the CSS file is generated by the PHP page using a simple <select> tag, which refers the chosen style-sheet using the syntax:
"index.php?file=". <select name="file"
onChange="self.location='index.php?file='+this.options[this.selectedIndex].value">

When an attacker provides a different file path to "index.php" page, it's possible to read any arbitrary file of the server, with the only limitation of web-server read permissions (enough to read /etc/passwd).

Instead, if an attacker provides a filename which not exists, the application will return some information about path of IMP and Apache on the server, like this:

```
Warning: Failed opening 'x' for inclusion  
(include_path='/usr/local/apache/php:.' in  
/var/data/horde/horde/admin/css/index.php on line 78
```

Exploit:

Using a lot of "../" in file path, it's possible to get off from web-root and read any file in the server. This is typical attack URL used to read passwd file of server:

<http://www.somesite.com/horde/admin/css/index.php?file=../../../../../../../../etc/passwd>

Using a non-existent filename, in this way, it's possible to exploit the path disclosure problem:

<http://www.somesite.com/horde/admin/css/index.php?file=xyyzz>

ADDITIONAL INFORMATION

The information has been provided by <mailto:eflorio@edmaster.it> Elia Florio.

=====

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.