[NEWS] Using data: URLs for Malware Injection (Opera)

Source: http://www.derkeiler.com/Mailing−Lists/Securiteam/2005−01/0055.html

---

From: SecuriTeam (*support_at_securiteam.com*)
Date: 01/12/05

```
To: list@securiteam.com
Date: 12 Jan 2005 11:56:33 +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/mailinglist.html

− − − − − − − − −

Using data: URLs for Malware Injection (Opera)
−−−

The attack works by using an URL scheme like this:
< a href="data:application/x−msdos−program;base64,[base64 data]">Click me!

Michael has made an example available which embeds putty.exe. The example is about 500 kByte HTML and is available on <http://kju.de/misc/putty.html> http://kju.de/misc/putty.html.

Michael's tests with various windows based webbrowsers had the following results:
* Internet Explorer 6 − Clicking on the link does nothing
* Mozilla version 1.5.4 − Will try to open the "what should I do with that" file dialog and then hangs. needs to get killed
* Firefox version 1.0 − Allows saving of the data to harddisk (on Linux it will also display much rubbish in the save dialog)
* Opera version 7.5.4 − Tells that it will open the file with notepad (which sounds ok), but will then EXECUTE IT INSTEAD (without further warning)

ADDITIONAL INFORMATION

The information has been provided by <mailto:kju−fd@fqdn.org> Michael Holzt.

==========

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.