

# [NT] Microsoft Windows VML Element Integer Overflow

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-01/msg00035.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 10 Jan 2007 16:09:27 +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>

-----

Microsoft Windows VML Element Integer Overflow

---

## SUMMARY

<<http://www.w3.org/TR/NOTE-VML>> VML is a component of the Extensible Markup Language (XML) that specifies vector images (e.g., rectangles and ovals). This functionality is implemented by the library "vgx.dll" in Microsoft Windows.

Successful exploitation of this vulnerability would allow an attacker to execute arbitrary code in the context of the user running the vulnerable application.

## DETAILS

### Vulnerable Systems:

- \* Internet Explorer 6.0 bundled with Windows XP SP2 with all available security patches is vulnerable.
- \* Other versions of Internet Explorer, including those with all security updates applied, are also vulnerable.
- \* Older versions of Internet Explorer may also be vulnerable.
- \* Microsoft Outlook with all available updates has been found to be vulnerable.

## [NT] Microsoft Windows VML Element Integer Overflow

\* Other Microsoft Office products, including Outlook, going back as far as Office 2000 may also vulnerable.

Remote exploitation of an integer overflow vulnerability in the Vector Markup Language (VML) support in multiple Microsoft products allows attackers to execute arbitrary code within the context of the user running the vulnerable application.

Exploitation would require an attacker to persuade a user to visit a malicious website using Internet Explorer, read a specially crafted e-mail message with Microsoft Outlook, or open a specially crafted document using an affected Microsoft Office application.

It is important to note that this vulnerability could be exploited without user interaction via an e-mail message when rendered within Outlook. For example, if a user with the reading pane turned on had Outlook open to an empty in-box when an attack e-mail arrived, exploitation could occur automatically.

This vulnerability exists due to insufficient input validation within vgx.dll. Two integer properties are multiplied together and no overflow check is performed. This could allow an attacker to force a memory allocation of a smaller amount of memory than is required. When copying user supplied data into the newly allocated memory, it is possible to overwrite a function pointer stored on the heap, which leads to the execution of arbitrary code.

Successful exploitation of this vulnerability would allow an attacker to execute arbitrary code in the context of the user running the vulnerable application.

Exploitation would require an attacker to persuade a user to visit a malicious website using Internet Explorer, read a specially crafted e-mail message with Microsoft Outlook, or open a specially crafted document using an affected Microsoft Office application.

It is important to note that this vulnerability could be exploited without user interaction via an e-mail message when rendered within Outlook. For example, if a user with the reading pane turned on had Outlook open to an empty in-box when an attack e-mail arrived, exploitation could occur automatically.

Workaround:

The following registry entry defines the library that implements the vulnerable functionality:

```
[HKEY_CLASSES_ROOT\CLSID\{10072CEC-8CC1-11D1-986E-00A0C955B42E}\InprocServer32]
```

Changing 'InprocServer32' in this registry entry to 'InprocServer32-disabled' causes the control that handles InprocServer32 not to load. Completely removing the key also provides the same protection.

## [NT] Microsoft Windows VML Element Integer Overflow

iDefence strongly recommends that users back up the registry before changing or removing this key.

It should also be noted that since the vulnerable component is not an ActiveX control, setting the kill bit does not disable the vulnerable DLL. As a result, setting the kill bit provides no protection against exploitation.

For previous vulnerabilities in this component, Microsoft suggested unregistering 'vgx.dll' on Windows XP SP1 and SP2 and Windows 2003 and 2003 SP1 systems. Using the "RegSvr32" program to unregister the dll in question with the following command also unregisters Vgx.dll:

```
regsvr32 -u "%ProgramFiles%\Common Files\Microsoft Shared\VGX\vgx.dll"
```

Alternatively, system administrators can deny "Full Access" to the file "%ProgramFiles%\Common Files\Microsoft Shared\VGX\vgx.dll".

The preceding workarounds will provide complete protection, but may prevent proper rendering of documents that rely on VML, such as Microsoft Word, Excel, and PowerPoint documents when saved in HTML format and viewed in IE or another application that uses the affected component. These documents can still be opened in the respective applications and will render correctly.

To mitigate the e-mail attack vector, Microsoft recommends that system administrators configure Outlook to view all e-mail messages in plain-text, including those from digitally signed "trusted" sources. Applying this workaround will prevent the rendering of rich content such as images and special formatting.

### Vendor Status:

Microsoft has addressed this vulnerability with Microsoft Security Bulletin  
<<http://www.microsoft.com/technet/security/bulletin/ms07-004.msp>>  
MS07-004.

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0024>>  
CVE-2007-0024

### Disclosure Timeline:

- \* 10-03-06 – Initial vendor notification
- \* 10-03-06 – Initial vendor response
- \* 01-09-07 – Coordinated public disclosure

## ADDITIONAL INFORMATION

The information has been provided by iDefence.  
The original article can be found at:

[NT] Microsoft Windows VML Element Integer Overflow

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=462>>  
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=462>

=====

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@xxxxxxxxxxxxxxxx

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

=====

=====

**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.