

[NT] Vulnerability in Microsoft OLE Dialog Allows Code Execution (MS07-011)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00041.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 15 Feb 2007 12:06:31 +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>

Vulnerability in Microsoft OLE Dialog Allows Code Execution (MS07-011)

SUMMARY

A remote code execution vulnerability exists in the OLE Dialog component provided with Microsoft Windows. An attacker could attempt to exploit this vulnerability when a user interacts with a malformed embedded OLE object within a Rich Text Format (RTF) file.

DETAILS

Affected Software:

* Microsoft Windows 2000 Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=7b1a81d5-1072-49d9-a24a-0e2630f62d8c>>

Download the update

* Microsoft Windows XP Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=e9b84661-25e3-4d38-95b1-8d3e7af565aa>>

Download the update

* Microsoft Windows XP Professional x64 Edition –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=57c1b19f-3242-457c-bedf-d35a8efe525c>>

Download the update

* Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1 –

[NT] Vulnerability in Microsoft OLE Dialog Allows Code Execution (MS07-011)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=eaed6f59-801e-45d7-9518-469d0de13cad>>

Download the update

* Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=cd1b18ae-bc8d-4d73-847f-4fa7ca672c88>>

Download the update

* Microsoft Windows Server 2003 x64 Edition –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=11f4f8f6-b8ce-4a5f-b7ed-8389ccc56473>>

Download the update

Non-Affected Software:

* Windows Vista

Mitigating Factors for OLE Dialog Memory Corruption Vulnerability – CVE-2007-0026:

* An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

* An attacker could only exploit this vulnerability when a user opens and then interacts with the embedded OLE object within an RTF file.

* This vulnerability could not be exploited automatically through a Web-based attack scenario. An attacker would have to host a Web site that contains an RTF file that is used to attempt to exploit this vulnerability. An attacker would have no way to force users to visit a malicious Web site. Instead, an attacker would have to persuade them to visit the Web site, typically by getting them to click a link that takes them to the attacker's site, and then convince the user to open the file.

* The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful a user must open an attachment that is sent in an e-mail message and then interact with the embedded OLE object within the RTF file.

Workarounds for OLE Dialog Memory Corruption Vulnerability – CVE-2007-0026:

Microsoft has tested the following workarounds. Although these workarounds will not correct the underlying vulnerability, they help block known attack vectors. When a workaround reduces functionality, it is identified in the following section.

* Enable Embedded Object blocking in Wordpad.exe

Note: This workaround only applies to Microsoft Windows XP Service Pack 2, Microsoft Windows Server 2003, and Microsoft Windows Server 2003 Service Pack 1 systems.

Wordpad.exe is the default application used to open Rich Text files. Users can temporarily block the parsing of embedded objects within Rich Text

[NT] Vulnerability in Microsoft OLE Dialog Allows Code Execution (MS07-011)

Files.

Warning If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

We recommend that you back up the registry before you edit it.

Use the following text to create a .reg file that will automate editing of the registry to temporarily block the parsing of embedded objects with Rich Text Files when using Wordpad.exe. You can copy the following text, paste it into a text editor such as Notepad, and then save the file with the .reg file name extension. Run the .reg file on the vulnerable client.

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\RtfStreamIn\ObjectBlocking\wordpad.exe]
```

Impact of Workaround: Wordpad.exe will no longer parse embedded objects within Rich Text files.

* Do not open or save RTF files that you receive from untrusted sources or that you receive unexpectedly from trusted sources. This vulnerability could be exploited when a user opens a specially crafted file.

* Un-install WordPad from Windows 2000 or Windows 2003

Wordpad.exe is the default application used to open Rich Text files. By uninstalling WordPad, users can block the parsing of embedded objects within Rich Text Files.

1. Click Start, click Control Panel, and then click Add or Remove Programs.
2. Click Add/Remove Windows Components, double-click Accessories and Utilities, and then double-click Accessories.
3. Uncheck Wordpad, click Okay to let the Optional Component manager uninstall Wordpad.

Impact of Workaround: Wordpad will no longer parse embedded objects within Rich Text files.

FAQ for OLE Dialog Memory Corruption Vulnerability – CVE-2007-0026:
What is the scope of the vulnerability?

A remote code execution vulnerability exists in the OLE Dialog component provided with Microsoft Windows. An attacker could exploit this vulnerability when a user interacts with a malformed embedded OLE object within a Rich Text Format (RTF) file. If a user were logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or

[NT] Vulnerability in Microsoft OLE Dialog Allows Code Execution (MS07-011)

create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative rights.

What is Rich Text Format (RTF)?

The Rich Text Format (RTF) Specification provides a format for text and graphics interchange that can be used with different output devices, operating environments, and operating systems.

What is OLE?

By using OLE technology, an application can provide embedding and linking support. OLE is the technology that applications use to create and edit compound documents. These are documents of one format, such as a Microsoft Word document, that contain embeddings of (or links to) documents of another format, such as Microsoft Excel. OLE 2.0 takes OLE even further by allowing in-place editing. Instead of launching a new application when an OLE object is activated, the user instead sees a new set of menu items inside their existing application. For more information about OLE, visit the following MSDN Web site.

What causes the vulnerability?

Windows OLE Dialog components do not perform sufficient validation when parsing OLE objects embedded within RTF files. When a user interacts with a malformed embedded OLE Object within an RTF file, it may corrupt system memory in such a way that an attacker could execute arbitrary code.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause arbitrary code to run with the privileges of the user who opened the file.

How could an attacker exploit the vulnerability?

An attacker could only exploit this vulnerability when a user opens and then interacts with the embedded OLE object within an RTF file.

This vulnerability could not be exploited automatically through a Web-based attack scenario. An attacker would have to host a Web site that contains an RTF file that is used to attempt to exploit this vulnerability. An attacker would have no way to force users to visit a malicious Web site. Instead, an attacker would have to persuade them to visit the Web site, typically by getting them to click a link that takes them to the attacker's site, and then convince the user to open the file.

The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful a user must open an attachment that is sent in an e-mail message and then interact with the embedded OLE object within the RTF file.

What systems are primarily at risk from the vulnerability?

Workstations and terminal servers are primarily at risk. Servers could be at more risk if administrators allow users to log on to servers and to run programs. However, best practices strongly discourage allowing this.

[NT] Vulnerability in Microsoft OLE Dialog Allows Code Execution (MS07-011)

What does the update do?

The update removes the vulnerability by modifying the way that the Windows OLE Dialog component parses OLE streams within RTF files.

When this security bulletin was issued, had this vulnerability been publicly disclosed?

No. Microsoft received information about this vulnerability through responsible disclosure. Microsoft had not received any information to indicate that this vulnerability had been publicly disclosed when this security bulletin was originally issued.

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?

No. Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Security Bulletin MS07-011.

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/ms07-011.msp>>
<http://www.microsoft.com/technet/security/bulletin/ms07-011.msp>

=====

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@xxxxxxxxxxxxxx

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

=====

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.