

Microsoft Internet Explorer Legacy Text Control Buffer Overflow (#NISR26082002)

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2002-08/0066.html>

From: NGSSoftware Insight Security Research (nisr@NEXTGENSS.COM)

Date: 08/26/02

Date: Mon, 26 Aug 2002 12:57:59 +0100
From: NGSSoftware Insight Security Research <nisr@NEXTGENSS.COM>
To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

NGSSoftware Insight Security Research Advisory

Name: Microsoft Internet Explorer BufferOverrun
Systems Affected: All versions IE
Severity: Critical
Category: Indirect Remote Buffer Overrun
Vendor URL: <http://www.microsoft.com>
Author: Mark Litchfield (mark@ngssoftware.com)
Date: 26th August 2002
Advisory number: #NISR26082002

Description

Microsoft® ActiveX® controls, formerly known as OLE controls or OCX controls, are components (or objects) you can insert into a Web page or other application to reuse packaged functionality someone else programmed. Whether you use an ActiveX control (formerly called an OLE control) or a Java object, Microsoft Visual Basic Scripting Edition and Microsoft Internet Explorer handle it the same way.

Details

An unchecked buffer exists in the ActiveX control used to display specially formatted text. This could be executed by encouraging an unsuspecting user to visit a malicious web page including the below code.

```
<OBJECT
  classid="clsid:99B42120-6EC7-11CF-A6C7-00AA00A47DD2"
  id=lblActiveLbl
  width=250
  height=250
  align=left
  hspace=20
```

NT-Bugtraq: Microsoft Internet Explorer Legacy Text Control Buffer Overflow (#NISR26082002)

```
vspace=0
>
<PARAM NAME="Angle" VALUE="90">
<PARAM NAME="Alignment" VALUE="4">
<PARAM NAME="BackStyle" VALUE="0">
<PARAM NAME="Caption" VALUE="long char string">
<PARAM NAME="FontName" VALUE="NGS Software Font">
<PARAM NAME="FontSize" VALUE="50">
<PARAM NAME="FontBold" VALUE="1">
<PARAM NAME="FrColor" VALUE="0">
</OBJECT>
```

By supplying an overly long value for the "Caption" parameter a saved return address stored on the stack will be overwritten allowing an attacker to gain control of Internet Explorer's path of execution. Any arbitrary code would execute in the context of the logged on user. By sending the intended target a specially crafted e-mail or by enticing them to a malicious website an attacker will be able to gain remote control of that users desktop.

Fix Information

NGSSoftware alerted Microsoft to these problems on the 29th April 2002.
NGSSoftware highly recommend installing Microsoft Patch found at
<http://www.microsoft.com/windows/ie/downloads/critical/q323759ie/default.asp>

Further Information

For further information about the scope and effects of buffer overflows,
please see

<http://www.ngssoftware.com/papers/non-stack-bo-windows.pdf>
<http://www.ngssoftware.com/papers/ntbufferoverflow.html>
<http://www.ngssoftware.com/papers/bufferoverflowpaper.rtf>
<http://www.ngssoftware.com/papers/unicodebo.pdf>

- **Previous message:** http-equiv@excite.com: "Terrible: Windows Media Player"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)