

CERT Advisory CA-2002-04 Buffer Overflow in Microsoft Internet Explorer

Source: <http://www.derkeiler.com/Mailing-Lists/Cert/2002-02/0003.html>

From: CERT Advisory (cert-advisory@cert.org)

Date: 02/25/02

Date: Mon, 25 Feb 2002 12:00:58 -0500 (EST)
From: CERT Advisory <cert-advisory@cert.org>
To: cert-advisory@cert.org

-----BEGIN PGP SIGNED MESSAGE-----

CERT Advisory CA-2002-04 Buffer Overflow in Microsoft Internet Explorer

Original release date: February 25, 2002

Last revised: --

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- * Microsoft Internet Explorer
- * Microsoft Outlook and Outlook Express
- * Other applications that use the Internet Explorer HTML rendering engine

Overview

Microsoft Internet Explorer contains a buffer overflow vulnerability in its handling of embedded objects in HTML documents. This vulnerability could allow an attacker to execute arbitrary code on the victim's system when the victim visits a web page or views an HTML email message.

I. Description

Internet Explorer supports the <EMBED> directive, which can be used to include arbitrary objects in HTML documents. Common types of embedded objects include multimedia files, Java applets, and ActiveX controls. The SRC attribute specifies the source path and filename of an object. For example, a MIDI sound might be embedded in a web page with the following HTML code:

```
<EMBED TYPE="audio/midi" SRC="/path/sound.mid" AUTOSTART="true">
```

Internet Explorer uses attributes of the <EMBED> directive and MIME information from the web server to determine how to handle an embedded object. In most cases, a separate application or plugin is used.

A g