

Re: O UT LO OK E XPRE SS 6 .00 : broken

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-02/0300.html>

From: Thor Larholm (thor@pivx.com)

Date: 02/24/03

From: "Thor Larholm" <thor@pivx.com>
To: <bugtraq@securityfocus.com>
Date: Mon, 24 Feb 2003 02:14:01 +0100

Outlook Express is not the only vulnerable product.

The culprit here is the codebase localPath vulnerability which was patched in Internet Explorer by MS02-015 in March 2002. GreyMagic had more fun with this at <http://security.greymagic.com/adv/gm001-ie/> which is also the origin of the example displayed.

MS02-015 crippled codeBase quite severely in Internet Explorer, completely removing most of its functionality in the Internet Zone. It is still possible to use this vulnerability in Internet Explorer in any local security zone, but getting to that zone in the first place is in itself an obstacle.

Whatever Microsoft patched in MS02-015 (crippling codeBase in the Internet Zone to avoid the command execution vulnerability) was only applied to the IE-specific parts of MSHTML and not to any shared parts that thirdparty programs such as Outlook and Outlook Express utilize. This despite our impression that MS02-015 removed the problem.

This is apparent if you examine Outlook 2000 which can also execute arbitrary commands automatically upon reading mails if you have set the security zone to the Internet Zone – just like Outlook Express as displayed by http-equiv

The default security zone for Outlook 2000 is the Internet Zone. It is first after you apply Office 2000 Service Pack 3 that the default zone is changed to the Restricted zone, so remember either to apply O2KSP3 or manually change your zone settings to Restricted at your earliest convenience.

Does Eudora still use the Internet Zone for viewing HTML mail? If so, it is also still vulnerable to the codeBase command execution vulnerability, like any other application that is embedding MSHTML.

Regards

Thor Larholm

PivX Solutions, LLC – Senior Security Researcher

SecurityFocus Bugtraq: Re: O UT LO OK E XPRE SS 6 .00 : broken

Latest PivX research: Multi-Vendor Unreal Engine Advisory
http://www.pivx.com/press_releases/ueng-adv_pr.html

----- Original Message -----

From: "http-equiv@excite.com" <http-equiv@MALWARE.COM>

To: <NTBUGTRAO@LISTSERV.NTBUGTRAO.COM>

Sent: Saturday, February 22, 2003 4:36 PM

Subject: O UT LO OK E XPRE SS 6 .00 : broken

> *Saturday, February 22, 2003*

>

> *Technical silent delivery and installation of an executable no client*

> *input other than reading an email or viewing a newsgroup message.*

> *Outlook Express 6.00 SP1 Cumulative Pack 1 2 3 4 whatever.*

Rest of original http-equiv post at

[http://www.ntbugtraq.com/default.asp?pid=36&sid=1&A2=ind0302&L=ntbugtraq&F=P
&S=&P=5888](http://www.ntbugtraq.com/default.asp?pid=36&sid=1&A2=ind0302&L=ntbugtraq&F=P&S=&P=5888)

The rest was snipped to avoid barking from premenstrual antivirus scanners.

Re: O UT LO OK E XPRE SS 6 .00 : broken