

Re: Microsoft Internet Explorer %USERPROFILE% Folder Disclosure Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-06/0012.html>

From: Russ (*Russ.Cooper_at_RC.ON.CA*)

Date: 06/05/03

Date: Thu, 5 Jun 2003 16:31:22 -0400

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Almost 400 of you responded to various addresses associated with the list automatically that the last message from Eiji Yoshida was a virus (I don't know how many he actually received, probably lots given how broken email products are.) See below for what products thought what, but they all felt there was an attachment...when there wasn't...and they all thought it was a virus...which it wasn't. The message is in the archives if you want to see what triggered it.

Between this and the numerous times when people install email AV brand new (and then scan their mail systems and send me hundreds of reports that NTBugtraq messages have viruses) it gets a little frustrating. I wish the AV Vendors did a better job of identifying actual exploit code from example code, but hey...;-[

Anyway, just wanted to let you know that your systems may be preventing you from receiving some useful security information, which you choose to receive. Its also worth trying to remember to prevent new AV installations on email systems from sending out alerts about messages that are 4 years old (or 4 days old for that matter, if you must send responses to viruses received, send them due to new messages.)

I'd put the archive link in here but then some anti-spam users would likely send it back to me as spam (I've had hundreds of spam reports based on the TruSecure Intellishield ad on the bottom of messages, seems there's something evil about URLs which contain the word offer or a mix of numbers and letters.)

It'll take me a little while to get those of you who erroneously responded removed, but I'm working on it. I don't need to see LSoft black-holed or have my mailbox flooded with erroneous virus alerts.

Antigen = 155 = Found "Unknown" that could not be cleaned.

Domino = 29 = "The file attachment / embedded was infected and not cleaned."

eManager = 5 = "Content filter has detected a message containing HTML script file."

WebShiled = 82 = "detected virus <x> in attachment unknown"

Unknown = 41

GroupShield = 78 =

Attachment Details:-

Attachment Name: N/A

File: Infected.msg

Infected? Yes

Repaired? No

Blocked? No

Deleted? Yes

NT-Bugtraq: Re: Microsoft Internet Explorer %USERPROFILE% Folder Disclosure Vulnerability

Virus Name: <I'm not telling...;-]>

Cheers,

Russ - NTBugtraq Editor