From: Ben Slivka
Sent: Sunday, April 13, 1997 2:23 PM
To: Bob Bejan
Subject: RE: Serious security holes in ActiveX controls for MSN (and elsewhere)

You're welcome. Please don't spread too broadly, we don't want this to leak out!

-----Original Message-----
From: **Bob Bejan**
Sent: Friday, April 11, 1997 10:08 PM
To: Ben Slivka
Subject: RE: Serious security holes in ActiveX controls for MSN (and elsewhere)

thanks for sending this ben...am making my team aware.

b.

-----Original Message-----
From: Ben Slivka
Sent: Thursday, April 10, 1997 11:57 AM
To: Tod Nielsen; Bob Bejan; Brad Chase; Rich Tong; Bob Muglia (Exchange); Erich Andersen (LCA)
Cc: Paul Maritz; Brad Silverberg; Jim Allchin (Exchange); John Ludwig; David Cole
Subject: FW: Serious security holes in ActiveX controls for MSN (and elsewhere)
Importance: High

Yikes, a big pile of doo-doo just waiting for someone to figure this out, and we will have the 2+ million MSN customers stepping in it...

-----Original Message-----
From: **Robert Welland**
Sent: Thursday, April 10, 1997 11:23 AM
To: Philip Bogle; Ben Slivka; Chris Jones; Bob Atkinson (Exchange)
Cc: Michael Toutonghi; Cornelius Willis; Brad Schick; Larry Sullivan
Subject: RE: Serious security holes in ActiveX controls for MSN (and elsewhere)
Importance: High

This is a really grim situation. Note that this is far worse then exploder because vicious behavior can simply leverage, presumably, "good" controls. The user has NO idea that they are undermining security when they install an improperly marked control from a reputable vendor. Authenticode has done its job - the vendor has not. The fact that Microsoft has improperly marked controls sets a very bad example.

The ability of scripts to blindly instanciate controls is VERY dangerous. We need a better security model then this. It is not clear to me what that correct model should be. However, it seems clear that a control should be able to limit the set of URLs that can instanciate it. This would probably solve the Norton and MSN problems. It will not solve the problems caused by general control vendors (who want wide distribution of their controls).

Each time one of these problems pops up I become more convinced that ActiveX is indefensible. It is clear that control vendors, including ourselves, are far too naïve about security to be trusted to make such powerful security policy decisions. Authenticode makes these decisions that much worse because the "goodness" of the brand name obscures the "badness" of the control. I would have been happier if these mistakes where inadvertent but it is clear that people are intentionally marking insecure behavior as safe. This is the worse possible scenario.

Bob Welland

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

Plaintiff's Exhibit

9089

Comes V. Microsoft

From: Philip Bogle
Sent: Thursday, April 10, 1997 6:25 AM
To: Robert Welland; Ben Slivka; Chris Jones
Cc: Michael Toutonghi; Cornelius Willis; Brad Schick; Larry Sullivan
Subject: Serious security holes in ActiveX controls for MSN (and elsewhere)
Importance: High

After hearing about the security hole in the Norton navigator control, I decided to review the security of other ActiveX controls likely to be preinstalled on users machine.

What I found is pretty shocking-- developers often sign and publish inherently unsafe or incorrectly marked controls, and Microsoft is one of the worst offenders.

Consider MSN, for example. It preinstalls several powerful and unsafe controls, nonetheless marked "Safe for Scripting". I created several web pages (attached below) that use these controls to munge the registry and accomplish other evils. Regardless of security settings, the MSN user gets absolutely no warning or chance to reject the controls before the damage is done (because MSN preinstalls them.)

Even without scripting, many controls are inherently dangerous. In a brief search of www.activex.com, I found three signed controls with the ability to run arbitrary unsigned code on the users machine without requiring any scripting and without any warnings to users. I have attached descriptions of these controls below.

Norton was not an isolated incident. We really have a general problem-- ActiveX control developers are behaving extremely naively with respect to security. They are creating signed controls with automated capabilities far too dangerous for general internet use, or marking controls "Safe for Scripting" that clearly shouldn't be, despite the pains we took to explain the meaning of that concepts. At this rate, ActiveX is going to gain an extremely bad reputation.

Below are the descriptions of the insecure controls...

MSN Registry Control
The web page below uses the "MSN Registry Control" (!!!) to inspect and modify keys in the various MSN subtrees of the registry. (It doesn"t allow arbitrary registry munging, but even the current capability is enough to cause serious trouble.) The example I created displays and/or deletes the MSN registry entries that list the URLs that the user has typed in.
<< File: hack-msn >>
A script using the control could do many more evil things: render components of MSN unusable by blowing away the appropriate registry entries, substitute a bogus stock server for the real one, fill up the users hard drive by creating registry keys ad infinitum, etc.

MSN Mail Control
This page uses the MSN mail control to obtain the user ID (which it could send back to the server) and to launch mail.

<< File: hack-mail >>
Active Data Connecter (possibly dangerous)
The Active Data Connector is marked "Safe for Scripting", and appears to allow a script on an untrusted page to connect to a database behind a firewall (as long as its not password protected) and siphon data out of it. I didn't come up with an example page, but someone who knows more about the ADC should think carefully about this

Below are controls that are dangerous even without scripting, which I found on www.activex.com.

DataRamp Assistant
"The DataRamp Assistant makes it easy to embed application references in World Wide Web pages. When a user clicks on a Web page, the DataRamp Assistant ActiveX control automatically downloads the application definition files, configures the required data source, and launches the application"

http://www.activex.com/PC/Result/TitleDetail/0,16,0-15818,00.html

Net-Installer
This controls allows programs to download and run automatically on the users machine

http://www.twenty.com/Pages/NI/NIDTK.shtml

App-launcher
This control supports the ability to launch arbitrary apps without user intervention.

http://www.activex.com/PC/Result/Download/0,27,0-22413,00.html