CERT Incident Note IN-2003-04: Exploitation of Internet Explorer Vulnerability

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community.

Exploitation of Internet Explorer Vulnerability

Original release Date: October 1, 2003
Last revised: October 4, 2003

Overview

The CERT/CC has received reports indicating that attackers are actively exploiting the Microsoft Internet Explorer vulnerability described in VU#865940.

Description

Reports to the CERT/CC indicate that attackers are leveraging the vulnerability described in VU#865940 to cause victim systems to perform various tasks. These attacks include the installation of tools for launching distributed denial-of-service (DDoS) attacks, reading sensitve information from the Windows registry, and the use of the victim system's modem to dial pay-per-minute services thereby incurring significant expense to users. Another attack known as "QHosts" misdirects network traffic by modifying Domain Name System (DNS) settings. By convincing a user running a vulnerable version of Microsoft Internet Explorer (IE) to view an HTML document (e.g., a web page or HTML email), a remote attacker could execute arbitrary code with the privileges of the user.

The vulnerability described in VU#865940 exists due to an interaction between IE's MIME type processing and the way it handles HTML application (HTA) files embedded in OBJECT tags. When an HTA file is referenced by the DATA attribute of an OBJECT element, and the web server returns the Content-Type header set to application/hta, IE may execute the HTA file directly, without user intervention. The HTML used to reference the HTA file can be created in at least three ways:

1. The HTML can be static
2. The HTML can be generated by script
3. The HTML can be generated by Data Binding an XML source to an HTML consumer

The extension of the HTA file does not affect this behavior, for example <OBJECT DATA="somefile.jpg"> (where somefile.jpg is a text file containing HTML code). IE security zone settings for ActiveX controls may prevent an HTA from being executed in this manner.

Additional details on VU#865940 can be found in the Vulnerability Note.

Any program that uses the WebBrowser ActiveX control or the IE HTML rendering engine (MSHTML) may be affected by this vulnerability. Outlook and Outlook Express are affected, however recent versions of these programs open mail in the Restricted sites zone where ActiveX controls and plug-ins are disabled by default.

Although Microsoft released a cumulative patch for Internet Explorer (see MS03-032) that stops HTAs from executing in one case in which static HTML is used to create an OBJECT element referencing the HTA, the patch did **not** prevent HTAs from executing in the cases when the requisite HTML is generated by script or by Data Binding. We have confirmed reports of attackers exploiting the Data Binding method. Microsoft has subsequently released security bulletin MS03-040 which supercedes MS03-032 and references a patch (828750) that purportedly fixes the cases where the HTML is generated by script or Data Binding.

Solutions

The CERT/CC is unaware of a complete solution for this vulnerability.

Apply patch

The cumulative patch (822925) referenced in Microsoft Security Bulletin MS03-032 (released on 2003-08-20) stops HTAs from executing in one case in which static HTML is used to create an OBJECT element referencing the HTA (1). The patch does **not** prevent HTAs from executing in at least two other cases in which the requisite HTML is generated by script (2) or by Data Binding (3). Microsoft has since released a new cumulative patch (828750), referenced in Microsoft Security Bulletin MS03-040 that fixes the latter cases. The CERT/CC recommends that users and administrators apply the patches from MS03-040 and consider taking the additional steps outlined below.

Additional steps for users

Disable ActiveX controls and plug-ins

It appears that disabling the "Run ActiveX controls and plug-ins" setting will prevent OBJECT elements from being instantiated, thus preventing exploitation of this vulnerability. Disable "Run ActiveX controls and plug-ins" in the Internet zone and any zone used to read HTML email. Note that there may be other attack vectors that are not governed by the "Run ActiveX controls and plug-ins" setting.

Apply the Outlook Email Security Update

Another way to effectively disable ActiveX controls and plug-ins in Outlook is to install the Outlook Email Security Update. The update configures Outlook to open email messages in the Restricted Sites Zone, where Active scripting is disabled by default. In addition, the update provides further protection against malicious code that attempts to propagate via Outlook. The Outlook Email Security Update is available for Outlook 98 and Outlook 2000. The functionality of the Outlook Email Security Update is included in Outlook 2002 and Outlook Express 6.

Maintain updated antivirus software

Antivirus software with updated virus definitions may identify and prevent some exploit attempts. Variations of exploits or attack vectors may not be detected. Do not rely on antivirus software to defend against this vulnerability. The CERT/CC maintains a partial list of antivirus vendors.

Additional steps for system administrators

The following steps are recommended for system administrators and advanced users.

Unmap HTA MIME type

Deleting or renaming the following registry key prevents HTAs from executing in the three cases listed above:

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\MIME\Database\Content Type\application/hta

Note that there may be other attack vectors that do not rely on this MIME setting.

Block Content-Type headers

Use an application layer firewall, HTTP proxy, or similar technology to block or modify HTTP Content-Type headers with the value "application/hta". This technique may not work for encrypted HTTP connections and it may break applications that require the "application/hta" Content-Type header.

Block mshta.exe

Use a host-based firewall to deny network access to the HTA host: %SystemRoot%\system32\mshta.exe. Examining network traces of known attack vectors, it seems that the exploit HTML/HTA code is accessed three times, twice by IE and once by mshta.exe. The HTA is instantiated at some point before the third access attempt. Blocking mshta.exe prevents the third access attempt, which appears prevent the exploit code from being loaded into the HTA. There may be other attack vectors that circumvent this workaround. For example, a vulnerability that allowed data in the browser cache to be loaded into the HTA could remove the need for mshta.exe to access the network. This technique may break applications that require HTAs to access the network. Also, specific host-based firewalls may or may not properly block mshta.exe from accessing the network.

Recovering from a system compromise

If you believe a system under your administrative control has been compromised, please follow the Steps for Recovering from a UNIX or NT System Compromise.

Reporting

The CERT/CC is tracking activity related to this vulnerability as CERT#35432. Relevant artifacts or reports can be sent to cert@cert.org with the appropriate CERT# in the subject line.

Authors: Allen Householder, Art Manion, and Chad Dougherty

Revision History

October 1, 2003: Initial release
October 4, 2003: Added information pertaining to MS03-040, noted registry and QHosts attacks