

Alert: Microsoft Security Bulletin – MS03–032

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-08/0091.html>

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

Date: 08/20/03

Date: Wed, 20 Aug 2003 13:56:28 -0400

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

<http://www.microsoft.com/technet/security/bulletin/MS03-032.asp>

Cumulative Patch for Internet Explorer (822925)

Originally posted: August 20, 2003

Summary

Who should read this bulletin: Customers using Microsoft® Internet Explorer.

Impact of vulnerability: Two new vulnerabilities, the most serious of which could enable an attacker to run arbitrary code on a user's system if the user either browsed to a hostile Web site or opened a specially crafted HTML-based email message.

Maximum Severity Rating: Critical

Recommendation: System administrators should install the patch immediately.

Affected Software:

- Microsoft Internet Explorer 5.01
- Microsoft Internet Explorer 5.5
- Microsoft Internet Explorer 6.0
- Microsoft Internet Explorer 6.0 for Windows Server 2003

An End User version of the bulletin is available at:

http://www.microsoft.com/security/security_bulletins/ms03-032.asp.

Technical description:

This is a cumulative patch that includes the functionality of all previously released patches for Internet Explorer 5.01, 5.5 and 6.0. In addition, it eliminates the following newly discovered vulnerabilities:

- A vulnerability involving the cross-domain security model of Internet Explorer, which keeps windows of different domains from sharing information. This flaw could result in the execution of script in the My Computer zone. To exploit this flaw, an attacker would have to host a malicious Web site that contained a Web page designed to exploit this particular vulnerability and then persuade a user to visit that site. After the user has visited the malicious Web site, it would be possible for the attacker to run malicious script by misusing the method Internet Explorer uses to retrieve files from the browser cache, and cause that script to

NT–Bugtraq: Alert: Microsoft Security Bulletin – MS03–032

access information in a different domain. In the worst case, this could enable the Web site operator to load malicious script code onto a user's system in the security context of the My Computer zone. In addition, this flaw could also enable an attacker to run an executable file that was already present on the local system or view files on the computer. The flaw exists because a file from the Internet or intranet with a maliciously constructed URL can appear in the browser cache running in the My Computer zone.

– A vulnerability that occurs because Internet Explorer does not properly determine an object type returned from a Web server. It could be possible for an attacker who exploited this vulnerability to run arbitrary code on a user's system. If a user visited an attacker's Web site, it would be possible for the attacker to exploit this vulnerability without any other user action. An attacker could also craft an HTML–based e–mail that would attempt to exploit this vulnerability.

This patch also sets the Kill Bit on the BR549.DLL ActiveX control. This control implemented support for the Windows Reporting Tool, which is no longer supported by Internet Explorer. The control has been found to contain a security vulnerability. To protect customers who have this control installed, the patch prevents the control from running or from being reintroduced onto users' systems by setting the Kill Bit for this control. This issue is discussed further in Microsoft Knowledge Base article 822925.

In addition to these vulnerabilities, a change has been made to the way Internet Explorer renders HTML files. This change addresses a flaw in the way Internet Explorer renders Web pages that could cause the browser or Outlook Express to fail. Internet Explorer does not properly render an input type tag. A user visiting an attacker's Web site could allow the attacker to exploit the vulnerability by viewing the site. In addition, an attacker could craft a specially formed HTML–based e–mail that could cause Outlook Express to fail when the e–mail was opened or previewed.

This patch also contains a modification to the fix for the Object Type vulnerability (CAN–2003–0344) corrected in Microsoft Security Bulletin MS03–020. The modification corrects the behavior of the fix to prevent the attack on specific languages.

To exploit these flaws, the attacker would have to create a specially formed HTML–based e–mail and send it to the user. Alternatively an attacker would have to host a malicious Web site that contained a Web page designed to exploit these vulnerabilities. The attacker would then have to persuade a user to visit that site.

As with the previous Internet Explorer cumulative patches released with bulletins MS03–004, MS03–015, and MS03–020 this cumulative patch will cause window.showHelp() to cease to function if you have not applied the HTML Help update. If you have installed the updated HTML Help control from Knowledge Base article 811630, you will still be able to use HTML Help functionality after applying this patch.

Mitigating factors:

- By default, Internet Explorer on Windows Server 2003 runs in Enhanced Security Configuration. This default configuration of Internet Explorer blocks these attacks. If Internet Explorer Enhanced Security Configuration has been disabled, the protections put in place that prevent these vulnerabilities from being exploited would be removed.
- In the Web–based attack scenario, the attacker would have to host a Web site that contained a Web page used to exploit these vulnerabilities. An attacker would have no way to force users to visit a malicious Web site outside the HTML–based e–mail vector. Instead, the attacker would need to lure them there, typically by getting them to click a link that would take them to the attacker's site.
- Code that executed on the system would only run under the privileges of the logged–on user.

Vulnerability identifier:

- BR549.DLL Buffer Overrun:CAN–2003–0530
- Browser Cache Script Execution in My Computer Zone:CAN–2003–0531

