Information Bulletin IB04-003 *February 02, 2004*

Microsoft Security Release (MS04-004)

Overview

Monday, February 02, 2004: Microsoft has released an accumulative patch supporting several previously identified vulnerabilities within Internet Explorer (IE). The vulnerabilities were first identified in 2003 and have been widely publicized through various open source forums. The Microsoft has given the advisory a “Critical” rating.

Brief description of Microsoft Security Bulletins

The security ratings are as assigned by the Vendor:

Critical

Microsoft Security Bulletin MS04-004

Microsoft Internet Explorer subframe cross-site scripting:
Microsoft Internet Explorer is vulnerable to cross-site scripting. By creating a malicious Web page that contains a subframe, a FRAME or IFRAME tag, the attacker could bypass the cross-domain security model. This could allow an attacker to cause the execution of malicious script within the victim's "My Computer" security zone, once the page is visited.

Microsoft Internet Explorer drag and drop could allow an attacker to save file to local system:
Microsoft Internet Explorer could allow a remote attacker to save a file to a target location on the victim's system, without the dialog box that asks for the victim's approval for the download being displayed. The drag and drop operations fail to properly validate specific Dynamic HTML (DHTML) events. A remote attacker could create a specially-crafted URL link, which would cause a malicious file to be saved to a target location on the victim's system, once the link is clicked. An attacker could exploit this vulnerability by creating a malicious Web page and hosting it on a Web site or by sending it to a victim as an HTML email.

Microsoft Internet Explorer domain URL spoofing:
Microsoft Internet Explorer could allow a remote attacker to spoof a trusted Web page by altering the URL that is displayed in the Internet Explorer address bar. A remote attacker could add a 0x01 character after the ampersand (@) in (http://user@domain), which would cause only part of the URL to be displayed in the address bar. An attacker could use this vulnerability to gain sensitive information from unsuspecting users, if they could be convinced to visit the spoofed site.

Microsoft Security Bulletin Breakout
The following is currently available for review on the Microsoft Security Website:

Microsoft Security Bulletin	Severity Rating	Link
MS04-004	Critical	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/Bulletin/ms04-004.asp

ISS X-Force Security Alerts
The following are currently available for review on the Internet Security Systems X-Force™ Website:

ISS X-Force Alert	Severity Rating	Link
Microsoft Internet Explorer subframe cross-site scripting	Medium Risk	http://xforce.iss.net/xforce/xfdb/13846
Microsoft Internet Explorer drag and drop could allow an attacker to save file to local system	Medium Risk	http://xforce.iss.net/xforce/xfdb/13679
Microsoft Internet Explorer domain URL spoofing	Medium Risk	http://xforce.iss.net/xforce/xfdb/13935

Security Alerts
The following features are currently available on the mentioned Websites:

Source/ Vendor	Associated Security Alerts	Link
CERT	Vulnerability Note VU#652278, Microsoft Internet Explorer does not properly display URLs	http://www.kb.cert.org/vuls/id/652278
Secunia	Internet Explorer System Compromise Vulnerabilities	http://www.secunia.com/advisories/10289/
Secunia	Microsoft Internet Explorer Multiple Vulnerabilities	http://www.secunia.com/advisories/9711/

Additional References
The following are currently available for review on the Microsoft Website:

Microsoft Knowledge Base Articles & Advisories	Link
200351	http://support.microsoft.com/default.aspx?kbid=200351
833786	http://support.microsoft.com/?id=833786
834489	http://support.microsoft.com/default.aspx?scid=kb;%5bLN%5d;834489
MS03-048	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-048.asp