CERT-In Monthly Security Bulletin September 06

High Vulnerabilities

Microsoft	Title of Vulnerability	Discovery / Publish Date	CERT-In References & Patch Information
Microsoft Word	Microsoft Word Remote Code Execution Vulnerability	September 08, 2006	CIVN-2006-87
Microsoft Publisher	Microsoft Publisher Remote Code Execution Vulnerability	September 13, 2006	CIVN-2006-90
Microsoft Internet Explorer	Microsoft Internet Explorer "daxctle.ocx" KeyFrame Memory Corruption Vulnerability	September 15, 2006	CIVN-2006-91
Microsoft Internet Explorer	Microsoft Internet Explorer Vector Markup Language Code Execution Vulnerability	September 21, 2006	CIVN-2006-92
Microsoft Internet Explorer	Microsoft Internet Explorer WebViewFolderIcon Buffer Overflow Vulnerability	September 28, 2006	CIVN-2006-94
Database	**Title of Vulnerability**	**Discovery / Publish Date**	**CERT-In References & Patch Information**
MySQL	MySQL MaxDB WebDBM Database Name Handling Remote Buffer Overflow Vulnerability	September 02, 2006	CIVN-2006-86
Unix	**Title of Vulnerability**	**Discovery / Publish Date**	**CERT-In References & Patch Information**
Sendmail	Sendmail Long Header Denial of Service Vulnerability	September 02, 2006	CIVN-2006-85
PHP	Multiple vulnerabilities in PHP	September 26, 2006	CIAD-2006-35
linux	Multiple vulnerabilities in linux	September 14, 2006	CIAD-2006-31
Miscellaneous	**Title of Vulnerability**	**Discovery / Publish Date**	**CERT-In References & Patch Information**
Wireshark (Ethereal)	Multiple vulnerabilities in Wireshark (Ethereal®)	September 14, 2006	CIAD-2006-32
Mozilla	Multiple Vulnerabilities in Mozilla Products	September 18, 2006	CIAD-2006-33
Adobe Flash Player	Adobe Flash Player Multiple Vulnerabilities	September 14, 2006	CIAD-2006-30

Medium Vulnerabilities

Microsoft	Title of Vulnerability	Discovery / Publish Date	CERT-In References & Patch Information
Microsoft Windows	Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	September 13, 2006	CIVN-2006-88
Microsoft Windows	Microsoft Windows Indexing Service Cross Site Scripting Vulnerability	September 13, 2006	CIVN-2006-89
Database	**Title of Vulnerability**	**Discovery / Publish Date**	**CERT-In References & Patch Information**
MySQL	MySQL Multiple Restrictions Bypass Vulnerabilities	September 12, 2006	CIAD-2006-28
Unix	**Title of Vulnerability**	**Discovery / Publish Date**	**CERT-In References & Patch Information**
GnuPG	Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	September 13, 2006	CIVN-2006-88

OpenSSL	Multiple vulnerabilities in OpenSSL	September 29, 2006	CIAD-2006-36
gzip	Multiple vulnerabilities in gzip	September 21, 2006	CIAD-2006-34
Linux	Multiple Vulnerabilities in Linux	September 12, 2006	CIAD-2006-27
Linux kernel	Linux kernel multiple vulnerability	September 01, 2006	CVE-2004-2660 CVE-2006-1858 CVE-2006-2444 CVE-2006-2932 CVE-2006-2935 CVE-2006-2936 CVE-2006-3468 CVE-2006-3626
Webmin and Usermin	Webmin and Usermin Cross Site Scripting and Source Code Disclosure Vulnerabilities	September 01, 2006	CVE-2006-4542
Apache2	Apache2 security problems	September 08, 2006	CVE-2005-2700
usermin	usermin: programming error	September 14, 2006	CVE-2006-4246
OpenSSH	OpenSSH Identical Blocks Denial of Service Vulnerability	September 28, 2006	CIVN-2006-93

Malicious Code Threats

Title of Malicious Code	Type	Overview	Aliases	Discovery Date	References
Trojan.Mdropper.Q	Worm	It is a Trojan horse that drops another threat on the compromised computer. The Trojan exploits an unpatched vulnerability in Microsoft Word 2000.	No Alias	September 1, 2006	http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2006-090219-2855-99
W32.Areses.Q@mm	Worm	It is a mass-mailing worm that opens a random tcp back door on the compromised computer and may download malicious files.	No Alias	September 5, 2006	http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2006-090611-4944-99&tabid=1
Banbra Trojan	Trojan	Trojan is targeting users of certain online banking service that uses virtual keyboards for their online operations.	No Alias	September 5, 2006	http://www.cert-in.org.in/virus/banbra.htm
Infostealer.Banigo	Trojan	It is a Trojan horse that steals confidential information from the affected computer. The stolen information	No Alias	September 22, 2006	http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2006-092211-2633-99

		may be related to financial Web sites. It also drops a rootkit to hide its presenceon the affected system.			
Stration Worm	Worm	The Stration worm is a mass mailing worm propagates by sending its copies in the attachment to email messages using their own SMTP engine. The worm obtain email addresses to send mail from Windows Address Book. Some variants are capable of sending emails without using any application such as Microsoft Outlook.	WORM_STRATIO.MY, WORM_STRATIO.QW, WORM_STRATIO.QL, WORM_STRATIO.QD, WORM_STRATION.WO (aliases AntiVir Worm/Stration.C, BitDefender Win32.Warezov.AT@mm, ClamAV Worm.Stration.CQ, Command W32/Warezov.AU, Dr Web Win32.HLLM.Limar.based, eSafe Win32.Stration.wo, eTrust-INO Win32/Stration.Variant!Worm, eTrust-INO (BETA) Win32/Stration.Variant!Worm, F-Prot W32/Warezov.AU, McAfee(BETA) W32/Stration@MM.dr, Nod32 Win32/Stration.EB worm, Panda(BETA) W32/Spamta.CY.worm, Sophos W32/Stratio-AN, Symantec(BETA) W32.Stration@mm, VirusBuster Trojan.Opnis.Gen!Pac2, WebWasher Worm.Stration.C), WORM_STRATION.BB, WORM_STRATION.AZ, WORM_STRATION.BH, WORM_STRATION.F, WORM_STRATION.A	September 30, 2006	http://www.cert-in.org.in/virus/stration.htm