Product Support Notice

PSN# PSN001642u

Original publication date: 29-Oct-2007. This is Issue #1, published 29-Oct-2007. Severity/risk level Medium Urgency Immediately

Name of problem Modular Messaging 3.1 Microsoft Patch List.

Products affected

Modular Messaging 3.1

Problem description

Avaya applies a set of Microsoft patches as part of the base installation of Modular Messaging installed in the factory. The majority of these patches are security updates.

Resolution

The following are included in the base software for MM 3.1:

Common Name	KB Article Number	Type	Description
MS03-026	823980	Security	Buffer Overrun in RPC
MS05-026	896358	Security	Privately reported vulnerability
MS05-027	901214	Security	Vulnerability in Windows Color Imaging
MS05-033	896428	Security	Vulnerability in Telnet client could allow information disclosure
MS05-038	896727		Cumulative security update for Internet Explorer - WindowsServer2003-KB896727-x86-ENU.exe
MS05-039	899588	Security	Privately reported Vulnerability in SMB
MS05-040	893756	Security	Privately reported Vulnerability in TAPI
MS05-041	899591	Security	Privately reported vulnerability in Terminal Services RDP
MS05-042	899587	Security	Privately reported vulnerability in Kerberos
MS05-045	905414	Security	Publicly reported vulnerability in Network Connections Service
MS05-048	901017	Security	Vulnerability in the Microsoft Collaboration Data Objects could allow code execution (Windows)
MS05-049	900725	Security	Privately reported vulnerability in Shell
MS05-050	904706	Security	Privately reported vulnerability in DirectShow Could Allow Remote Code
MS05-051	902400	Security	Privately reported vulnerability in Com+/ Microsoft Distributed Transaction Coordinator (MSDTC)
MS05-052	899528		Cumulative security update for Internet Explorer - WindowsServer2003-KB899528-x86-ENU
MS05-053	896424	Security	Privately reported vulnerability in Win32 Graphics Device Interface (GDI) and Extended MetaFile (EMF)
MS06-001	912919	Security	Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution
MS06-002	908519	Security	Vulnerability in Embedded Web Fonts Could Allow Remote Code Execution
MS06-008	911927	Security	Vulnerability in Web Client Service Could Allow Remote Code Execution
MS06-009	901190	Security	Vulnerability in the Korean Input Method Editor Could Allow Elevation of Privilege
MS06-014	911562	Security	Publicly reported vulnerabilities in MDAC
MS06-015	908531	Security	Security Update for Shell
MS06-022	918439	Security	Vulnerability in ART Image Rendering Could Allow Remote Code Execution
MS06-024	917734	Security	Vulnerability in Windows Media Player Could Allow Remote Code Execution

MS06-025	911280	Security	Vulnerability in Routing and Remote Access Could Allow Remote Code Execution
MS06-032	917953	Security	Vulnerability in TCP/IP Could Allow Remote Code Execution
MS06-034	917537	Security	Privately reported vulnerability in IIS
MS06-036	914388	Security	Privately reported vulnerability in DHCP
MS06-040	921883	Security	Vulnerability in Server Service Could Allow Remote Code Execution
MS06-041	920683	Security	Vulnerabilities in DNS Resolution Could Allow Remote Code Execution
MS06-045	921398	Security	Vulnerability in Windows Explorer Could Allow Remote Code Execution
MS06-046	922616	Security	Vulnerability in HTML Help Could Allow Remote Code Execution
MS06-050	920670	Security	Vulnerabilities in Microsoft Windows Hyperlink Object Library Could Allow Remote Code Execution
MS06-051	917422	Security	Vulnerability in Windows Kernel Could Result in Remote Code Execution
MS06-051	917422	Security	Vulnerability in Windows Kernel Could Result in Remote Code Execution
MS06-053	920685	Security	Vulnerability in Indexing Service Could Allow Cross-Site Scripting
MS06-057	923191	Security	Vulnerability in Windows Shell Could Allow Remote Code Execution
MS06-061	924191	Security	Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution
MS06-063	923414	Security	Vulnerability in Server Service Could Allow Denial of Service
MS06-064	922819	Security	Vulnerabilities in TCP/IP Could Allow Denial of Service
MS06-065	924496	Security	Vulnerability In Windows Object Packager Could Allow Remote Code Execution
MS06-066	923980	Security	Vulnerabilities in Client Service for NetWare Could Allow Remote Code Execution
MS06-068	920213	Security	Vulnerability in Microsoft Agent Could Allow remote Code Execution
MS06-072	925454	Security	Affecting: Windows 2000, Windows 2003, Windows XP
MS06-074	926247	Security	Affecting: Windows 2000, Windows 2003, Windows XP
MS06-076	923694	Security	Affecting: Windows 2000, Windows 2003, Windows XP
MS06-078	923689	Security	Vulnerability in Windows Media Format Could Allow Remote Code Execution
MS06-78	925398	Security	Vulnerability in Windows Media Format could allow remote code execution
Netware Client Service	899589	Security	Privately reported vulnerability in Netware Client Service
Windows Update Client	910437	Security	Non-security update for Windows Update Client
	890830		The Microsoft Windows Malicious Software Removal Tool helps remove specific, prevalent malicious software from computers that are running Windows Vista, Windows Server 2003, Windows XP, or Windows 2000
	898715		An update for Windows Installer 3.1 is available for Windows Server 2003 SP1 and for the 64-bit editions of Windows XP
	911897		Files are corrupted on a Windows Server 2003-based computer when you try to use the local UNC path to copy the files
	922582		Error message when you try to update a Microsoft Windows-based computer: "0x80070002"
	928388		2007 time zone update for Windows XP and Windows Server 2003 - WindowsServer2003-KB928388-x86-ENU.exe

Workaround or alternative remediation

n/a

Remarks

n/a

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch	
n/a	
Download	
n/a	
Patch install instructions	**Service-interrupting?**
n/a	No
Verification	
n/a	
Failure	
n/a	
Patch uninstall instructions	
n/a	

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks
n/a
Avaya Security Vulnerability Classification
Not Susceptible
Mitigation
n/a

For additional support, contact your Authorized Service Provider. Depending on your coverage entitlements, additional support may incur charges. Support is provided per your warranty or service contract terms unless otherwise specified.

Avaya Support Contact	Telephone
U.S. Remote Technical Services – Enterprise	800-242-2121
U.S. Remote Technical Services – Small Medium Enterprise	800-628-2888
U.S. Remote Technical Services – BusinessPartners for Enterprise Product	877-295-0099
BusinessPartners for Small Medium Product	Please contact your distributor.
Canada	800-387-4268
Caribbean and Latin America	786-331-0860
Europe, Middle East, and Africa	36-1238-8334
Asia Pacific	65-6872-8686