

TopResponse Threat Advisory

Release Date: October 16, 2008

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Host Integration Server RPC Vulnerability (MS08-059,CVE-2008-3466).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Host Integration Server SP2, 2000, 2004 (Server), 2004 (Client), 2004 SP1, 2006 for 32-bit systems, 2006 for x64-based systems.

Alert Type: Critical vulnerability

Risk Assessment: Moderate

Threat Impact: Remotely exploitable vulnerability that could allow an attacker to control vulnerable systems

Advisory Impact: Prevention

Summary: Microsoft Host Integration Server (HIS) is a gateway application that supports connectivity between Microsoft Windows and IBM mainframe AS/400 systems. The application provides support for APPC, SNA, 3270, CICS and other IBM protocols. The application also provides support for advanced integration with Microsoft Windows networks and software, including Microsoft DTC, Microsoft MSMQ, and cross-platform access to DB2 databases. The application supports communication between server and management workstations using the DCE-RPC protocol system. The reported vulnerability could allow an attacker to execute arbitrary code on the users systems in the context of the logged-on user by sending a specially crafted DCE-RPC request.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2008-10-14-03 (or later) to put this new protection into place. This is automatically applied to the "Recommended Client Protection" and "Recommended Server Protection" IPS Rule Sets. In order to take advantage of the protection, make sure the IPS rule tln-106202 is enabled in the IPS Rule Set used to inspect traffic to your Microsoft Host Integration Server infrastructure.

References: Use the following sources for additional information:

Additional Information	Location
Top Layer Support Web site	http://www.toplayer.com/support
Microsoft Advisory	http://www.microsoft.com/technet/security/bulletin/MS08-059.mspx

Relevant TLN Rules: tln-106202

Relevant TopResponse Protection Pack(s): 2008-10-14-03