

TopResponse Threat Advisory

Release Date: February 9, 2011

Purpose: The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide proactive protection for the Microsoft IIS FTP Service Heap Buffer Overrun Vulnerability (MS11-004,CVE-2010-3972).

Top Layer Products: IPS 5500 and higher.

Vulnerable Infrastructure: Microsoft FTP Service 7.0 for IIS 7.0 when installed on Windows Vista Service Pack 1 and Windows Vista Service Pack 2, Microsoft FTP Service 7.5 for IIS 7.0 when installed on Windows Vista Service Pack 1 and Windows Vista Service Pack 2, Microsoft FTP Service 7.0 for IIS 7.0 when installed on Windows Vista x64 Edition Service Pack 1 and Windows Vista x64 Edition Service Pack 2, Microsoft FTP Service 7.5 for IIS 7.0 when installed on Windows Vista x64 Edition Service Pack 1 and Windows Vista x64 Edition Service Pack 2, Microsoft FTP Service 7.0 for IIS 7.0 when installed on Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems Service Pack 2, Microsoft Internet Information Services 7.5 on Windows Server 2008 R2 for Itanium-based Systems, and other software versions as specified in the Microsoft advisory for the vulnerability.

Alert Type: Critical vulnerabilities

Risk Assessment: Critical

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

Advisory Impact: Prevention

Summary: Microsoft Internet Information Service (IIS) implements support for FTP using the FTP service. There exists a vulnerability in the way the Microsoft IIS FTP service processes incoming commands. The reported vulnerabilities could allow a remote attacker to execute arbitrary code on the systems running the Microsoft IIS FTP service by sending a specially crafted FTP request. The IPS 5500 provides proactive protection for this vulnerability.

Recommended Action: Top Layer recommends the following actions:

Ensure that the rule tln-004003, “PROTO: FTP Command Too Long”, is enabled in the IPS Rule Set that is used to inspect traffic sent to your Microsoft IIS FTP Server infrastructure. The rule is currently enabled in the “Recommended Client Protection” and “Recommended Server Protection” IPS Rule Sets.

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/MS11-004.msp

Relevant TLN Rules: tln-004003.