

TopResponse Threat Advisory

Release Date: June 26, 2008

Purpose: The Top Layer TopResponse team is issuing this advisory, which provides information needed to block attacks targeting the Microsoft Frontpage Extensions Information Disclosure and Microsoft Frontpage Extensions Path Disclosure Vulnerabilities and provide detection capabilities for attempts to access phpMyAdmin infrastructure.

Top Layer Products: IPS 5500 4.x and later.

Vulnerable Infrastructure: Microsoft IIS v4.0, v5.0, phpMyAdmin v2.11.7 and earlier.

Alert Type: Information Disclosure Vulnerabilities

Risk Assessment: Low

Threat Impact: Remotely exploitable vulnerabilities that could allow an attacker to obtain sensitive information from vulnerable systems

Advisory Impact: Prevention

Summary: Microsoft Frontpage Extensions package is a set of server-side plug-ins included in IIS required to support content and publishing features. The reported vulnerabilities could allow an attacker to obtain details of the Microsoft Frontpage installation by sending a specially crafted request.

phpMyAdmin is an open-source tool designed to enable administration of MySQL over the Internet. The tool needs to be properly secured to ensure only authorized access is allowed, which requires the ability to detect remote attempts to access phpMyAdmin.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2008-06-24-05 (or later) to put this new protection into place. The Protection Pack adds two new rules tln-103047 and tln-103048 and modifies the existing rule tln-103038. The rules tln-103038 and tln-103047 are enabled in the "Recommended Server Protection" IPS Rules Set. The rule tln-103038 is enabled in the "Recommended Server Protection – Detect Only" IPS Rule Set. In order to take advantage of the protection, make sure the IPS rules tln-103038, tln-103047 are enabled in the IPS Rule Set used to inspect traffic to your Microsoft Frontpage infrastructure and the rule tln-103048 is enabled in the IPS Rule Set used to inspect traffic to your phpMyAdmin infrastructure.

References: Use the following sources for additional information:

Additional Information	Location
Top Layer Support Web site	http://www.toplayer.com/support
Microsoft Support Article	http://support.microsoft.com/kb/828909

Relevant TLN Rules: tln-103038, tln-103047, tln-103048.

Relevant TopResponse Protection Pack(s): 2008-06-24-05.