

TopResponse Threat Advisory

Release Date: October 5, 2007

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to block attacks for the Microsoft MFC FileFind Heap Overflow ActiveX Vulnerability (CVE-2007-4916).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Visual Studio 6.0, 2005, and .NET, and products embedding the vulnerable Microsoft component, including HP All-in-One Series Web Release and HP Photo & Imaging Gallery 1.1.

Alert Type: Critical Vulnerability

Risk Assessment: Critical

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

Advisory Impact: Prevention

Summary: The Microsoft Foundation Classes Library (MFC) is a library that makes portions of the Windows API available through C++ classes. The library is provided to third-party vendors to facilitate application development. There is a vulnerability in the CfileFind::FindFile() function implemented by the Microsoft library. Among the vendors using the vulnerable function is HP All-in-One Series Web Release and HP Photo & Imaging Gallery. This advisory addresses known attacks against the vulnerable Microsoft component in the vendor's software using the HTML vector. The reported vulnerability could allow an attacker to execute arbitrary code on the users systems in the security context of the logged-on user by enticing the user to open a specially crafted web page.

Recommended Action: Top Layer recommends the following actions:

IPS 5500 E-Series Users: Download and apply Protection Pack 2007-10-04-02 (or later) to put this new protection into place. This is automatically applied to the "Recommended Client Protection" IPS Rule Set. No further action is needed.

References: Use the following sources for additional information:

Additional Information	Location
Top Layer Support Web site	http://www.toplayer.com/support
CERT Advisory	http://www.kb.cert.org/vuls/id/611008

Relevant TLN Rules: TLN-106169

Relevant TopResponse Protection Pack(s): 2007-10-04-02