

TopResponse Threat Advisory

Release Date: June 9, 2010

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Internet Explorer v8 Developer Tools Vulnerability (MS10-034, CVE-2010-0811).

Top Layer Products: IPS 5500 E-Series running V5.18.002 (or later).

Vulnerable Infrastructure: Microsoft Internet Explorer v8 Developer Tools ActiveX Control.

Alert Type: Critical Vulnerability

Risk Assessment: Critical

Threat Impact: Remotely exploitable vulnerability that could allow an attacker to write or delete arbitrary files on the vulnerable systems

Advisory Impact: Prevention

Summary: The Microsoft Internet Explorer v8 Developer Tools ActiveX Control provides web application developers a method to debug behavior specific to Internet Explorer. The vulnerability could allow an attacker to execute arbitrary code on the user's system in the 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:

Download and apply Protection Pack 2010-06-08-01 (or later) to put this new protection into place. This protection is automatically applied to the "Recommended Client Protection" IPS Rule Set. In order to take advantage of the protection, customers should make sure the IPS rule tln-106315, "EXPLT: Microsoft Internet Explorer v8 Developer Tools Vulnerability", is enabled in the IPS Rule Set used to inspect traffic that transfers HTML traffic to your infrastructure which may have the vulnerable tool set installed.

Note: In order to take advantage of the protection provided by these rules, IPS 5500 software version V5.18.002 or higher is required.

References: Use the following sources for additional information:

| Additional Information | Location |
|-------------------------------|---|
| Top Layer Support | http://www.toplayer.com/support |
| Microsoft Support | http://www.microsoft.com/technet/security/bulletin/ms10-034.msp |
| Mitre CVE | http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0811 |

Relevant TLN Rules: tln-106315

Relevant TopResponse Protection Pack: 2010-06-08-01

Relevant Top Layer Software Version(s): V5.18.002 or later