



## OutsideView™ Security Bulletin September, 2009

**THREAT:** Microsoft™ has released an emergency patch to protect against a discovered threat of information disclosure or remote code execution, arising from vulnerabilities in their Visual Studio Active Template Library (ATL). There have been attacks that target this vulnerability.

**APPLICABILITY:** ActiveX controls created by any developers using affected versions of MS Visual Studio are potentially vulnerable. Microsoft has tested Visual Studio 2003, 2005, and 2008 and found them to be vulnerable. Versions of Visual Studio earlier than 2003 were not tested, so their level of vulnerability is unknown.

**MICROSOFT REMEDIATION:** Microsoft has released critical patch (MS09-034) for all versions of IE to protect consumers, along with a security update for Visual Studio (MS09-035) to help developers fix the controls and components they built that could be affected.

### OUTSIDEVIEW:

**VERSION 8.X:** Crystal Point has reacted rapidly to this Microsoft security vulnerability. OutsideView 8.0 “c” maintenance update has been analyzed and a suspect single component (in a third-party library) subject to the Microsoft security vulnerability has been removed as it was un-needed for OutsideView functionality.. OutsideView 8.0c is, therefore, now **MS09-035 compliant** and no longer subject to this remote code execution threat.

It is strongly recommended that all users of OutsideView 8.0, 8.0a and 8.0b upgrade to 8.0c. To facilitate this update, Crystal Point will provide all licensed users of OutsideView 8.0 with an update to OutsideView 8.0c at no charge.

**PRIOR VERSIONS:** OutsideView 7.3 and earlier used Visual Studio versions that have not been tested by Microsoft for this vulnerability. The vulnerability of earlier OutsideView release is therefore unknown, but suspect. It is recommended that all versions of OutsideView be upgraded to 8.0c as well.

For technical questions please email [support@crystalpoint.com](mailto:support@crystalpoint.com)

For sales please email [Sales@crystalpoint.com](mailto:Sales@crystalpoint.com)

For additional technical detail:

<http://www.microsoft.com/technet/security/bulletin/ms09-035.mspx>

<http://www.microsoft.com/technet/security/bulletin/MS09-037.mspx>

<http://www.microsoft.com/technet/security/bulletin/ms09-034.mspx>

<http://www.microsoft.com/technet/security/advisory/973882.mspx>

[http://voices.washingtonpost.com/securityfix/2009/07/microsofts\\_emergency\\_patch\\_mes.html?wprss=securityfix](http://voices.washingtonpost.com/securityfix/2009/07/microsofts_emergency_patch_mes.html?wprss=securityfix)