Vulnerability Advisory

Name	ChemviewX ActiveX Multiple Stack Overflows
Date Released	February 11th 2010
Affected Software	ChemView ActiveX v1.9.5
Researcher	Paul Craig paul.craig@security-assessment.com

Description

Hyleos ChemviewX is a free ActiveX control used to visualize chemical structures from MDL or MOL files.
The ClassID of the object is {C372350A-1D5A-44DC-A759-767FC553D96C} and the control is marked safe for scripting.

Two stack overflows were discovered in the control, both overflow conditions can be used to gain command execution.

Exploitation

The methods SaveasMolFile and ReadMolFile are both vulnerable to a stack overflow condition which can be reached when supplying more than 400 white-space characters in the filename argument. Both tab and space characters can be used to trigger the overflow condition.
The 401-404th byte will result in the overflow of the return pointer. This vulnerability can be used to gain command execution when combined with a JavaScript heap spray by jumping into a pre-allocated heap.

Vendor Advice and Recommendations
The vendor was contacted multiple times over a two month period without any response. Use of this control is not suggested.
If you use this ActiveX control consider setting the kill bit for the control's Classid ({C372350A-1D5A-44DC-A759-767FC553D96C}), or uninstall the control.

About Security-Assessment.com

Security-Assessment.com is Australasia's leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

Web   www.security-assessment.com
Email   info@security-assessment.com