

13 July 2009

By: Marius Oiaga, Technology News Editor

[Microsoft Warns of Office Web Components 0-Day](#)

A fix is already available



Office
Microsoft

Customers running various releases of the Office System will need to take the necessary precautions in order to bulletproof their computers against exploits targeting a zero-day vulnerability affecting Office Web Components, Microsoft warned. According to the Redmond company, limited, active attacks have been detected in the wild. In the eventuality of a successful exploit of the Spreadsheet ActiveX control vulnerability, a potential attacker would have similar user rights as the local user.

"Our investigation has shown that although Internet Explorer (IE) isn't vulnerable, remote code execution is possible and may not require any user intervention when using IE. This ActiveX Control has been deprecated for some time but we still recommend that all customers implement the workarounds outlined in the security advisory to help prevent the control from loading in IE until a security update is available," revealed Dave Forstrom, group manager of the Trustworthy Computing group.

Although a security update is in the works, Microsoft does have a fix already in place addressing the issue. In [Security Advisory 973472](#), under the Workarounds section users will be able to find the necessary steps that need to be taken in order to render exploits useless. Not fond of the manual implementation of the workaround? Well, the software giant also provides an automatic method for delivering the fix via [Knowledge Base Article 973472](#). Users need to only navigate to the specific KB article and hit the Fix It button.

"Microsoft has activated its Software Security Incident Response Process (SSIRP) and continues to investigate this vulnerability. Microsoft is currently working to develop a security update to address this vulnerability and will release it once it has reached an appropriate level of quality for broad distribution," Forstrom added.

Microsoft enumerated the products impacted by the vulnerability: Office XP SP3, Office 2003 SP3, Office XP Web Components SP3, Office Web Components 2003 SP3, Office 2003 Web Components for the 2007 Microsoft Office system SP1, Internet Security and Acceleration Server 2004 Standard Edition SP3, Internet Security and Acceleration Server 2004 Enterprise Edition SP3, Internet Security and Acceleration Server 2006, Internet Security and Acceleration Server 2006 Supportability Update, Internet Security and Acceleration Server 2006 SP1, Office Small Business Accounting 2006.