
Security Advisory Summary

Dec 15, 2010

The security advisory summary below lists advisories issued between **Nov 10, 2010** and **Dec 15, 2010**. This list is compiled by the Security Management Team based on the notices we receive from numerous reputable resources including, but not limited to, the product vendors, [Multi-State Information Sharing and Analysis Center](#) (MS-ISAC) and [United States Computer Emergency Readiness Team](#) (US-CERT).

Updating computer platforms to fix security vulnerabilities wherever possible is a security policy requirement. Please ensure testing and implementation happens within your respective environments as soon as possible. If there are any problems please send an email to tenn.update.services@state.tn.us.

December 2010		
Number	Date Issued	Subject
2010-107	Tuesday, December 14, 2010	Multiple vulnerabilities in Microsoft Office Publisher Could Allow Remote Code Execution (MS10-103)
2010-106	Tuesday, December 14, 2010	Vulnerabilities in Microsoft Office Graphics Filters Could Allow for Remote Code Execution (MS10-105)
2010-105	Tuesday, December 14, 2010	Vulnerabilities in the OpenType Font (OTF) Driver Could Allow Remote Code Execution (MS10-091)
2010-104	Tuesday, December 14, 2010	Multiple Vulnerabilities in Internet Explorer Could Allow Remote Code Execution (MS10-090)
2010-097	Tuesday, December 14, 2010	Vulnerability in Internet Explorer Could Allow

		Remote Code Execution
2010-103	Friday, December 10, 2010	Multiple Vulnerabilities in Mozilla Products Could Allow Remote Code Execution
2010-100	Friday, December 10, 2010	Multiple Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (MS10-087)
2010-102	Wednesday, December 08, 2010	Multiple Vulnerabilities in Apple QuickTime Player Could Allow Remote Code Execution

November 2010		
Number	Date Issued	Subject
2010-095	Tuesday, November 16, 2010	Vulnerability in Multiple Adobe Products Could Allow Remote Code Execution
2010-101	Friday, November 12, 2010	Multiple Vulnerabilities in Apple Mac OS X Could Allow Remote Code Execution

Certain entries have been grouped to provide a more coherent picture of the development of certain vulnerabilities and related corrective actions.

Should one need to take a corrective action, please follow up by reading the information pointed to by the related links. Please be aware that, though many patches are cumulative, some aren't, and are dependent on the installation of previous updates.