

State of Tennessee

Department of Finance and Administration
Office for Information Resources
Security Policy and Audit



Security Advisory Summary JUNE 9, 2010

The Security Advisory Summary below lists advisories issued between **MAY 12, 2010** and **JUNE 8, 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, the [Multi-State Information Sharing and Analysis Center](#) (MS-ISAC), and the [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 you identify any issues or know of any potential problems please send an email to tenn.update.services@state.tn.us.

Vendor	Date	Rating	Title	URL	Affected Software
Adobe	May 12, 2010	High	Adobe has released a security update to address multiple vulnerabilities in Adobe Shockwave Player 11.5.6.606 and earlier versions for both Windows and Macintosh operating systems. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code.	http://www.adobe.com/support/security/bulletins/apsb10-12.html	Adobe Shockwave Player 11.5.6.606
Cisco	May 13, 2010		Cisco has released updates to address multiple vulnerabilities in Cisco PGW Softswitch. These vulnerabilities may allow an attacker to cause a denial-of-service condition.	http://www.cisco.com/en/US/products/products_security_advisory09186a0080b2c519.shtml	Cisco PGW Softswitch
Apple	May 19, 2010		Updates for Java Mac OS X 10.5 and 10.6	http://support.apple.com/kb/HT4170 http://support.apple.com/kb/HT4171	Java Mac OS X 10.5 and 10.6
Google	May 26, 2010		Google has released Chrome 5.0.375.55 for Linux, Mac, and Windows to address multiple vulnerabilities. These vulnerabilities may allow an attacker to bypass security restrictions, execute script in an unsafe context, or mislead users.	http://googlechromereleases.blogspot.com/2010/05/stable-channel-update.html	Earlier versions of Chrome 5.0.375.55
Google	June 9, 2010		Google has released Chrome 5.0.375.70 for Linux, Mac, and Windows to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code, conduct cross-site scripting attacks, bypass security restrictions, or obtain sensitive information.	http://googlechromereleases.blogspot.com/2010/06/stable-channel-update.html	Earlier versions of Chrome 5.0.375.70

Security Advisory Summary – March 10, 2010

Vendor	Date	Rating	Title	URL	Affected Software
Cisco	May 27, 2010		Cisco has released a security advisory to address multiple vulnerabilities in Network Building Manager. The advisory indicates that the legacy Richards-Zeta Mediator products are also affected by these vulnerabilities. Exploitation of these vulnerabilities may allow an attacker to operate with escalated privileges or obtain sensitive information.	http://www.cisco.com/en/US/products/products_security_advisory09186a0080b2c518.shtml	Cisco Network Building Manager
Adobe	June 5, 2010		Adobe has released a security advisory to notify users of a vulnerability in Adobe Flash Player, Reader, and Acrobat. Exploitation of this vulnerability may allow an attacker to execute arbitrary code and take control of the affected system. The advisory indicates that Adobe is aware of active exploitation of this vulnerability.	http://www.adobe.com/support/security/advisories/apsa10-01.html	Adobe Flash Player, Reader, and Acrobat
Apple	June 8, 2010		Apple has released Safari 5.0 and Safari 4.1 for Windows and Mac OS X to address multiple vulnerabilities in ColorSync, Safari, and WebKit. These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, obtain sensitive information, or conduct cross-site scripting attacks.	http://support.apple.com/kb/HT4196	ColorSync, Safari, and WebKit
Microsoft	June 8, 2010		Microsoft has released updates to address vulnerabilities in Microsoft Windows, Internet Explorer, Office, SharePoint, and .NET Framework as part of the Microsoft Security Bulletin Summary for June 2010. These vulnerabilities may allow an attacker to execute arbitrary code or operate with elevated privileges.	http://www.microsoft.com/technet/security/bulletin/ms10-jun.mspx	Microsoft Windows, Internet Explorer, Office, SharePoint, and .NET Framework

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 are not and are dependent on the installation of previous updates.

Links of Special Cyber-Security Interest:

- <http://www.msisac.org/dashboard/>
- http://www.symantec.com/business/security_response/index.jsp
- <http://isc.sans.org/>