

State of Tennessee

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



Security Advisory Summary MAY 12, 2010

The security advisory summary below lists advisories issued between **APRIL 14, 2010** and **MAY 12, 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.

Vendor	Date	Rating	Title	URL	Affected Software
Cisco	April 15, 2010		Cisco has released a security advisory to address a vulnerability in Cisco Secure Desktop. Cisco Secure Desktop contains a vulnerable ActiveX control that may allow an attacker to execute arbitrary code.	http://www.cisco.com/en/US/products/products_security_advisory09186a0080b25d01.shtml	Cisco Secure Desktop
Apple	April 15, 2010		Apple has released security update 2010-003 to address a vulnerability in the ATS package. This vulnerability may allow an attacker to execute arbitrary code.	http://support.apple.com/kb/HT4131	Mac OS X v10.5.8, Mac OS X Server v10.5.8, Mac OS X v10.6.3, Mac OS X Server v10.6.3
Oracle	April 15, 2010	High	Multiple vulnerabilities have been discovered in the Oracle Java (formerly known as Sun Java) Runtime Environment (JRE) that could allow attackers to take complete control of a vulnerable system. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.	http://blogs.oracle.com/security/2010/04/security_alert_for_cve-2010-08.html	JRE 1.6 Update 10 - JRE 1.6 Update 19
Oracle	April 16, 2010		Oracle has released Sun Java SE 1.6.0_20 to address several vulnerabilities. The release notes for this version of Java SE indicate that these vulnerabilities are in Java Deployment Toolkit and the new Java Plug-in.	http://www.oracle.com/technology/deploy/security/alerts/alert-cve-2010-0886.html	Sun Java SE 1.6.0_20

Security Advisory Summary – March 10, 2010

Vendor	Date	Rating	Title	URL	Affected Software
HP	April 20, 2010	High	HP has issued a patch to remedy a vulnerability in HP Operations Manager. This vulnerability can be exploited if a user visits or is redirected to a specially crafted website designed to exploit this vulnerability. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.	http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02078800	HP Operations Manager for Windows v8.16 HP Operations Manager for Windows v8.10 HP Operations Manager for Windows v7.5
McAfee	April 21, 2010		The recent McAfee signatures are detecting svchost.exe as being infected with the "wecorl.a" virus. Once detected, the machine continuously reboots itself and may become unusable. It may also cause a Blue screen or DCOM error, followed by shutdown messages after updating to the 5958 DAT on April 21, 2010.	https://kc.mcafee.com/corporate/index?page=content&id=KB68780	McAfee 5958 DAT file for McAfee Antivirus software
McAfee	April 22, 2010		McAfee DAT release 5958 is incorrectly identifying the valid system file svchost.exe, as containing malicious code. Reports indicate that a false positive detection occurs on Windows XP Service Pack 3 systems. Users should apply the "extra.dat" and additional updates provided by McAfee as necessary to mitigate this issue. Users should ensure that they have installed DAT 5959 or greater before running any on-demand scans.	http://service.mcafee.com/FAQDocument.aspx?lc=&id=TS100969 https://kc.mcafee.com/corporate/index?page=content&id=KB68780&pmv=print http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=265240#none	McAfee 5959 DAT file for McAfee Antivirus software
Google	April 21, 2010		Google has released Chrome 4.1.249.1059 for Windows to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code, conduct cross-site scripting attacks, or conduct cross-site request forgery attacks.	http://googlechromereleases.blogspot.com/2010/04/stable-update-security-fixes.html	Google Chrome 4.1.249.1059 for Windows
Google	April 28, 2010		Google has released Chrome 4.1.249.1064 for Windows to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code or bypass the same origin policy in the	http://googlechromereleases.blogspot.com/2010/04/stable-update-bug-and-security-fixes.html	Google Chrome 4.1.249.1064 for Windows

Security Advisory Summary – March 10, 2010

Vendor	Date	Rating	Title	URL	Affected Software
			browser.		
VideoLAN	April 21, 2010		VideoLAN has released a security advisory to address multiple vulnerabilities in VLC Media Player. These vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition.	http://www.videolan.org/security/sa1003.html	VLC Media Player
Cisco	April 22, 2010		Cisco has released a security advisory to address a vulnerability that affects Cisco Small Business Video Surveillance Cameras and Cisco RVS4000 4-Port Gigabit Security Routers. This vulnerability may allow an unprivileged user to gain full administrative access on the device or obtain sensitive information.	http://www.cisco.com/warp/public/707/cisco-sa-20100421-vsc.shtml	Cisco Small Business Video Surveillance Cameras Cisco RVS4000 4-Port Gigabit Security Routers
Microsoft	April 23, 2010		The Microsoft Security Response Center has posted a blog entry indicating that it has revoked the update related to Microsoft security bulletin MS10-025 because it does not effectively correct the underlying vulnerability. This vulnerability affects Windows Media Services running on Windows 2000 Server. The blog entry indicates that Microsoft has targeted a re-release of the update for next week.	http://blogs.technet.com/msrc/default.aspx http://www.microsoft.com/technet/security/Bulletin/MS10-025.mspx	Windows Media Services on Windows 2000 Server
Microsoft	April 27, 2010		Microsoft has re-released the security update related to Microsoft security bulletin MS10-025. This vulnerability affects Windows Media Services running on Windows 2000 Server. The original release of this update had been revoked last week because it did not effectively correct the underlying vulnerability.	http://blogs.technet.com/msrc/archive/2010/04/27/ms10-025-re-release-ready.aspx http://www.microsoft.com/technet/security/bulletin/ms10-025.mspx	Windows Media Services on Windows 2000 Server
Microsoft	April 30, 2010		Microsoft has released security advisory 983438 to notify users of a vulnerability in Microsoft Windows SharePoint Services 3.0 and Microsoft Office SharePoint Server 2007. The advisory states that Microsoft is investigating public reports of exploitation of the vulnerability that may allow the execution of arbitrary script within the SharePoint site.	http://www.microsoft.com/technet/security/advisory/983438.mspx	Microsoft Windows SharePoint Services 3.0 Microsoft Office SharePoint Server 2007

Security Advisory Summary – March 10, 2010

Vendor	Date	Rating	Title	URL	Affected Software
Opera	April 30, 2010		Opera Software has released Opera 10.53 to address a vulnerability. Exploitation of this vulnerability may allow an attacker to execute arbitrary code.	http://www.opera.com/support/kb/view/953/	Opera 10.53
Foxit	May 5, 2010		The Foxit Corporation has released Foxit Reader 3.3 for Windows. This release of Foxit Reader contains a component called Trust Manager. Foxit Reader release notes indicate that the Trust Manager enables users to allow or deny unauthorized actions and data transmission, including URL connection, attachments PDF action, and JavaScript. This addresses the vulnerability in the PDF specification /Launch function.	http://www.foxitsoftware.com/pdf/reader/whatsnew33.htm	Foxit Reader 3.3 for Windows
Microsoft	May 6, 2010	High	Two new vulnerabilities have been discovered in the Microsoft SMTP (Simple Mail Transfer Protocol) service that could lead to the disclosure of information. Microsoft Windows SMTP service is a component that allows emails to be sent and received. These vulnerabilities could be exploited if an attacker creates a specially crafted query that is designed to exploit these vulnerabilities. This could allow an attacker to redirect network traffic which could lead to the unauthorized disclosure of information. Please note that both of these vulnerabilities were fixed by the patches referenced in MS10-024, dated April 13, 2010, but were not disclosed in this security bulletin.	http://www.microsoft.com/technet/security/Bulletin/MS10-024.mspx	Microsoft Windows 2000 Microsoft Windows XP Microsoft Windows 2003 Microsoft Windows 2008 Microsoft Exchange Server 2003 Microsoft Exchange Server 2007 Microsoft Exchange Server 2010
Apple	May 10, 2010		A vulnerability affecting Apple Safari has surfaced. By convincing a user to open a specially crafted web page, an attacker may be able to execute arbitrary code. Exploit code for this vulnerability is publicly available.	http://www.kb.cert.org/vuls/id/943165 http://www.us-cert.gov/reading_room/securing_browser/ http://www.us-cert.gov/current/index.html#apple_safari_vulnerability	Apple Safari

Security Advisory Summary – March 10, 2010

Vendor	Date	Rating	Title	URL	Affected Software
Microsoft	May 11, 2010		Microsoft has released updates to address vulnerabilities in Microsoft Windows, Office, and Visual Basic for Applications as part of the Microsoft Security Bulletin Summary for May 2010. These vulnerabilities may allow an attacker to execute arbitrary code.	http://www.microsoft.com/technet/security/bulletin/ms10-may.msp	Microsoft Outlook Express Microsoft Windows Mail Microsoft Windows Live Mail Microsoft Office Microsoft Visual Basic for Applications third-party software that uses Visual Basic for Applications
Adobe	May 12, 2010		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/psb10-12.html	Adobe Shockwave Player 11.5.6.606

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.

Additional Information and Follow Ups:

ZEUS/WALEDAC RELATED ISSUES AT STATE OF TENNESSEE

- Zeus/Waledac events at the state continue to be seen. As mentioned in the April Advisory Summary, these are being caused partly by the installation of certain toolbars, one possible offender being the "Shop-at-Home" toolbar, however some Zeus/Waledac events are being caused by actual infections. Please see the previous Advisory Summary for instructions on how to deal with this.
Some IHD tickets concerning this issue were given a certain timeframe with which to deal with this before the machines were blocked. Those blocks are being issued for those machines that are still exhibiting the behaviors listed above.
Thank you for your continued cooperation and vigilance.

Links of Special Cyber/Security Interest:

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