US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary

- May 2012 -

This report summarizes general activity including updates to the National Cyber Awareness System in May 2012. It includes current activity updates, alerts, and bulletins, in addition to other newsworthy events or highlights.

Executive Summary

During May 2012, US-CERT issued 11 Current Activity entries, one Alert, and four weekly Bulletins.

Highlights for this month include updates or advisories released by Microsoft, Google, Adobe, and Apple.

Contents

Current Activity

Current Activity entries are high-impact security threats and vulnerabilities currently reported to US-CERT. The following table lists all of the entries posted this month followed by a brief overview of the most significant entries.

Current Activity for May 2012	
May 1	Google Releases Chrome 18.0.1025.168
May 3	Microsoft Releases Advanced Notification for May Security Bulletin
May 4	Adobe Releases Security Advisory for Adobe Flash Player
May 8	Microsoft Releases May Security Bulletin
May 8	Apple Releases iOS 5.1.1
May 9	Adobe Releases Security Bulletins for Multiple Products
May 10	Apple Releases Multiple Security Updates
May 15	Apple Releases Flashback Malware Security Updates
May 15	Google Releases Google Chrome 19
May 16	Apple Releases QuickTime 7.7.2
May 24	Google Releases Google Chrome 19.0.1084.52

- Microsoft released updates to address vulnerabilities in Microsoft Windows, Office, .NET Framework, and Silverlight as part of the Microsoft Security Bulletin Summary for May 2012. These vulnerabilities may allow an attacker to execute arbitrary code or operate with elevated privileges. US-CERT encourages users and administrators to review the bulletin and follow best-practice security policies to determine which updates should be applied.
- Google released Chrome 18.0.1025.168, Chrome 19, and Chrome 19.0.1084.52 for Linux, Macintosh, Windows, and Google Chrome Frame to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition.
- Adobe released a Security Advisory for Adobe Flash Player to address a vulnerability that may allow an attacker to cause a denial-of-service condition or take control of the affected system. Affected software versions include the following:
    - Adobe Flash Player 11.2.202.233 and earlier versions for Windows, Macintosh, and Linux operating systems
    - Adobe Flash Player 11.1.115.7 and earlier versions for Android 4.x
    - Adobe Flash Player 11.1.111.8 and earlier versions for Android 3.x and 2.x
- Adobe released security bulletins to alert users of critical vulnerabilities in multiple products. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code or take control of an affected system. The following products are affected:
    - Adobe Illustrator CS 5.5 and earlier versions for Windows and Macintosh
    - Adobe Photoshop CS 5.5 and earlier versions for Windows and Macintosh
    - Adobe Flash Professional CS 5.5 (11.5.1.349) and earlier versions for Windows and Macintosh
    - Shockwave Player 11.6.4.634 and earlier versions for Windows and Macintosh
- Apple released updates for multiple products to address vulnerabilities.
    - iOS 5.1.1 for iPhone, iPod, iPad, and iPad 2 addressed multiple vulnerabilities that may allow an attacker to execute arbitrary code, perform a cross-site scripting attack, or spoof a website address.
    - Security updates for Apple OS X and Safari addressed multiple vulnerabilities that may allow an attacker to execute arbitrary code, obtain sensitive information, operate with elevated privileges, cause a denial-of-service condition, or perform a cross-site scripting attack.
    - QuickTime 7.7.2 addressed multiple vulnerabilities that may allow an attacker to execute arbitrary code or cause a denial-of-service condition.

Alerts

Alerts provide timely information about current security issues, vulnerabilities, and exploits.

Alerts for May 2012	
May 8	TA12-129A Microsoft Updates for Multiple Vulnerabilities

Bulletins

Bulletins are issued weekly and provide a summary of new vulnerabilities recorded by the National Institute of Standards and Technology's (NIST's) National Vulnerability Database (NVD). The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD)/US-CERT. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

Bulletins for May 2012	
May 8	SB12-128 Vulnerability Summary for the Week of April 30, 2012
May 14	SB12-135 Vulnerability Summary for the Week of May 7, 2012
May 21	SB12-142 Vulnerability Summary for the Week of May 14, 2012
May 29	SB12-149 Vulnerability Summary for the Week of May 21, 2012

A total of 426 vulnerabilities were recorded in the NVD during May 2012.

Security Highlights

Apple Releases Flashback Malware Security Updates

Apple has released security updates to address Flashback malware in the following products:

- OS X Lion v10.7.3
- OS X Lion Server v10.7.3
- Mac OS X v10.6.8
- Mac OS X Server v10.6.8

Apple has released a malware removal tool for the most common variants of the Flashback malware. If the malware is discovered, the tool will notify the user and remove it automatically. If the malware is not discovered, no indication will be given.

Update: On May 14, 2012, Apple released security updates to address Flashback malware in the following product:

- Mac OS X v10.5 to v10.5.8

US-CERT encourages users and administrators to review articles HT5247, HT5254, and HT5273 and apply any necessary updates to help mitigate the risk.

Contacting US-CERT

If you would like to contact US-CERT to ask a question, submit an incident, or learn more about cybersecurity, please use one of the methods listed below. If you would like to provide feedback on this report, or if you have comments or suggestions for future reports, please email info@us-cert.gov.

Website Address: http://www.us-cert.gov
Email Address: info@us-cert.gov
Phone Number: +1 (888) 282-0870
PGP Key ID: 0xEDA10949
PGP Key Fingerprint: 5A24 6040 50FC 1BA3 81FA 0919 1378 C036 EDA1 0949
PGP Key: https://www.us-cert.gov/pgp/info.asc