



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary - June 2009 -

This report summarizes general activity as well as updates made to the [National Cyber Alert System](#) for June 2009. This includes current activity updates, technical and non-technical cyber security alerts, cyber security bulletins, and cyber security tips, in addition to other newsworthy events or highlights.

Executive Summary

During June 2009, US-CERT issued 12 Current Activity entries, two (2) Technical Cyber Security Alerts, two (2) Cyber Security Alerts, five (5) weekly Cyber Security Bulletins, and one (1) Cyber Security Tip.

Highlights for this month include updates released by Microsoft, Apple, Mozilla, Adobe, Foxit, and spam campaigns related to the recent celebrity deaths.

Contents

Executive Summary	1
Current Activity	1
Technical Cyber Security Alerts	3
Cyber Security Alerts	3
Cyber Security Bulletins	3
Cyber Security Tips	3
Security Highlights	4
Contacting US-CERT	4

Current Activity

[Current Activity](#) entries are high-impact security threats and vulnerabilities currently being reported to US-CERT. The most significant entries of the month are highlighted below, followed by a table listing all of the entries posted this month.

- Microsoft has released an update to address vulnerabilities in Microsoft Windows, Office, and Internet Explorer as part of the Microsoft Security Bulletin Summary for [June 2009](#). These vulnerabilities may allow an attacker to execute arbitrary code, operate with elevated privileges, or obtain sensitive information. Additional information regarding these vulnerabilities can be found in Technical Cyber Security Alert [TA09-160A](#).
- Apple released multiple updates in June for iTunes, Quicktime, Safari, Java, and iPhone OS.
 - Apple has released iTunes 8.2 and QuickTime 7.6.2 to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition. Further details can be found in Apple articles [HT3592](#) and [HT3591](#).
 - [Safari 4.0](#) for Windows and Mac OS X addresses multiple vulnerabilities in CFNetwork, CoreGraphics, ImageIO, International Components for Unicode, libxml, Safari, Safari Windows Installer, and WebKit. These vulnerabilities may allow an attacker to execute

arbitrary code, cause a denial-of-service condition, obtain sensitive information, bypass security restrictions, or conduct cross-site scripting attacks. Further details are available in Apple article [HT3613](#).

- Apple released Java for Mac OS X 10.4 Release 9 and Java for Mac OS X 10.5 Update 4 to address multiple vulnerabilities in Java. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code. Details are described in Apple articles [HT3633](#) and [HT3632](#).
- Mozilla Foundation released Firefox 3.0.11 and 3.5 in June.
 - Mozilla Foundation released Firefox 3.0.11 to address multiple vulnerabilities that may allow an attacker to execute arbitrary code, mislead users, or obtain sensitive information. Many of these vulnerabilities also affect Thunderbird and SeaMonkey; however, updated versions of those packages are not currently available. Refer to the [Mozilla Foundation Security Advisories](#) released on June 11, 2009 for additional details.
 - Mozilla Foundation released [Firefox 3.5](#) with multiple security enhancements including improved anti-phishing, anti-malware, and privacy protection. The Firefox 3.5 [release notes](#) and [features](#) provide detailed information for this update.
- Adobe released Shockwave Player 11.5.0.600 to address a vulnerability that may allow a remote attacker to take control of an affected system. Further details are provided in Adobe security bulletin [APSB09-08](#).
- Foxit Reader has released updates for multiple vulnerabilities. By convincing a user to open a malicious PDF file, an attacker may be able to execute code or cause a vulnerable PDF viewer to crash. The PDF could be emailed as an attachment or hosted on a website. Additional information is provided in the [Foxit Security Bulletin](#) and US-CERT Vulnerability Note [VU#251793](#).

Current Activity for June 2009	
June 2	Apple Releases iTunes 8.2 and QuickTime 7.6.2
June 4	Microsoft Releases Advance Notification for June Security Bulletin
June 9	Apple Releases Safari 4.0
June 10	Microsoft Releases June Security Bulletin
June 10	Adobe Releases Security Updates for Adobe Reader and Acrobat
June 12	Mozilla Foundation Releases Firefox 3.0.11
June 16	Apple Releases Java Updates for Mac OS X 10.4 and 10.5
June 18	Apple Releases iPhone OS 3.0
June 23	Foxit Reader Contains Multiple Vulnerabilities
June 24	Adobe Releases Update for Shockwave Player
June 26	Spam, Phishing, and Malicious Code Related to Recent Celebrity Deaths
June 30	Mozilla Foundation Releases Firefox 3.5

Technical Cyber Security Alerts

[Technical Cyber Security Alerts](#) are distributed to provide timely information about current security issues, vulnerabilities, and exploits.

<i>Technical Cyber Security Alerts for June 2009</i>	
June 9	TA09-160A Microsoft Updates for Multiple Vulnerabilities
June 10	TA09-161A Adobe Acrobat and Reader Vulnerabilities

Cyber Security Alerts

[Cyber Security Alerts](#) are distributed to provide timely information about current security issues, vulnerabilities, and exploits. They outline the steps and actions that non-technical home and corporate users can take to protect themselves.

<i>Cyber Security Alerts (non-technical) for June 2009</i>	
June 9	SA09-160A Microsoft Updates for Multiple Vulnerabilities
June 10	SA09-161A Adobe Acrobat and Reader Vulnerabilities

Cyber Security Bulletins

[Cyber Security Bulletins](#) are issued weekly and provide a summary of new vulnerabilities recorded by the National Institute of Standards and Technology (NIST) [National Vulnerability Database \(NVD\)](#). The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSA) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

<i>Security Bulletins for June 2009</i>	
	SB09-152 Vulnerability Summary for the Week of May 25, 2009
	SB09-159 Vulnerability Summary for the Week of June 1, 2009
	SB09-166 Vulnerability Summary for the Week of June 8, 2009
	SB09-173 Vulnerability Summary for the Week of June 15, 2009
	SB09-180 Vulnerability Summary for the Week of June 22, 2009

A total of 451 vulnerabilities were recorded in the [NVD](#) during June 2009.

Cyber Security Tips

[Cyber Security Tips](#) are primarily intended for non-technical computer users and are issued monthly. June's tip focused on good security habits.

<i>Cyber Security Tips for June 2009</i>	
June 3	ST04-003 Good Security Habits
June 17	ST04-004 Understanding Firewalls
June 30	ST04-005 Understanding Anti-Virus Software

Security Highlights

Spam, Phishing, and Malicious Code Related to Recent Celebrity Deaths

US-CERT is aware of public reports of spam campaigns, phishing attacks, and malicious code targeting the recent deaths of Ed McMahon, Michael Jackson, Farrah Fawcett, and Billy Mays. These email messages may attempt to gain user information through phishing attacks or by recording email addresses if the user replies to the message. Additionally, email messages may contain malicious code or may contain a link to a seemingly legitimate website that contains malicious code.

US-CERT would like to remind users to remain cautious when receiving unsolicited email. Users are encouraged to take the following measures to protect themselves from these types of attacks:

- Do not follow unsolicited web links received in email messages.
- Install and maintain up-to-date antivirus software.
- Refer to the [Recognizing and Avoiding Email Scams](#) (pdf) document for more information on avoiding email scams.
- Refer to the [Avoiding Social Engineering and Phishing Attacks](#) document for more information on social engineering attacks.

Contacting US-CERT

If you would like to contact US-CERT to ask a question, submit an incident, or to learn more about cyber security, 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.

Web Site Address: <http://www.us-cert.gov>

Email Address: info@us-cert.gov

Phone Number: +1 (888) 282-0870

PGP Key ID: [CF5B48C2](#)

PGP Key Fingerprint: 01F1 9C58 0817 D612 45ED 3FCF 3004 FE8C CF5B 48C2

PGP Key: <https://www.us-cert.gov/pgp/info.asc>