



# US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

## Monthly Activity Summary - August 2009 -

This report summarizes general activity as well as updates made to the [National Cyber Alert System](#) for August 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 August 2009, US-CERT issued 14 Current Activity entries, two (2) Technical Cyber Security Alerts, two (2) Cyber Security Alerts, five (5) weekly Cyber Security Bulletins, and two (2) Cyber Security Tips.

Highlights for this month include multiple updates released by Adobe, Apple, Cisco, Microsoft, and Mozilla. Also, the fifth annual GFIRST national conference was held in August.

### Contents

<b>Executive Summary</b> .....	<b>1</b>
<b>Current Activity</b> .....	<b>1</b>
<b>Technical Cyber Security Alerts</b> .....	<b>3</b>
<b>Cyber Security Alerts</b> .....	<b>3</b>
<b>Cyber Security Bulletins</b> .....	<b>3</b>
<b>Cyber Security Tips</b> .....	<b>4</b>
<b>Security Highlights</b> .....	<b>4</b>
<b>Contacting US-CERT</b> .....	<b>5</b>

### 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.

<b>Current Activity for August 2009</b>	
<b>August 4</b>	<a href="#">Mozilla Releases Firefox 3.0.13 and Firefox 3.5.2</a>
<b>August 4</b>	<a href="#">Apple Releases iPhone OS 3.0.1</a>
<b>August 5</b>	<a href="#">Sun Releases Update 15 for Java SE 6</a>
<b>August 6</b>	<a href="#">Apple Releases Mac OS X v10.5.8 and Security Update 2009-003</a>
<b>August 6</b>	<a href="#">Microsoft Releases Advance Notification for August Security Bulletin</a>
<b>August 12</b>	<a href="#">Apple Releases Safari 4.0.3</a>
<b>August 12</b>	<a href="#">Microsoft Releases August Security Bulletin</a>

<b>Current Activity for August 2009</b>	
<b>August 18</b>	<a href="#">Adobe Releases Hotfixes for ColdFusion and JRun Vulnerabilities</a>
<b>August 19</b>	<a href="#">Cisco Releases Security Advisory for Firewall Services Module Vulnerability</a>
<b>August 21</b>	<a href="#">Libpurple Contains Remote Code Execution Vulnerability</a>
<b>August 21</b>	<a href="#">Adobe Releases Security Bulletin for Flex SDK</a>
<b>August 26</b>	<a href="#">Autonomy KeyView SDK Vulnerability</a>
<b>August 27</b>	<a href="#">Cisco Releases Security Advisory for Unified Communications Manager</a>
<b>August 31</b>	<a href="#">Microsoft Internet Information Services (IIS) FTP Service Vulnerability</a>

- Apple released updates for the iPhone OS, Mac OS X, and Safari during August.
  - Apple has released iPhone OS 3.0.1 to address a vulnerability in the CoreTelephony component. By sending a specially crafted SMS message to a user, an attacker may be able to execute arbitrary code or cause a denial-of-service condition. US-CERT encourages users to review Apple article [HT3754](#) and apply any necessary updates to help mitigate the risk.
  - Mac OS X v10.5.8 and Security Update 2009-003 addressed multiple vulnerabilities in a number of applications. These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, bypass security mechanisms, operate with escalated privileges, or obtain sensitive information. Additional information can be found in US-CERT Technical Cyber Security Alert [TA09-218A](#) and Apple article [HT3757](#).
  - Safari 4.0.3 for Windows and Mac OS X addressed multiple vulnerabilities that may allow an attacker to execute arbitrary code, cause a denial-of-service condition, obtain sensitive information, or spoof a website. Additional details can be found in Apple article [HT3733](#).
- Adobe released hot fixes for ColdFusion and JRun, along with a security bulletin for Flex SDK.
  - Adobe security bulletin [APSB09-13](#) addressed a vulnerability in Flex 3.3 SDK and earlier versions. This vulnerability may allow an attacker to conduct a cross-site scripting attack. The update also included the latest version of Adobe Flash Player.
  - Adobe released security bulletin [APSB09-12](#) to provide hotfixes for JRun 4.0 and ColdFusion 8.0.1 and earlier versions. These vulnerabilities may allow an attacker to execute arbitrary code, obtain sensitive information, or operate with escalated privileges.
- Cisco released security advisories for Firewall Services Module (FWSM) and Cisco Unified Communications Manager (CUCM).
  - Security Advisory [cisco-sa-20090819-fwsm](#) addressed a vulnerability in FWSM for the Catalyst 6500 series switches and the 7600 series routers. By sending specially crafted ICMP messages to the Firewall Services Module, an attacker could cause a denial-of-service condition.
  - Security Advisory [cisco-sa-20090826-cucm](#) addressed multiple vulnerabilities in CUCM. These vulnerabilities may allow a remote attacker to cause a denial-of-service condition.
- Microsoft released an update to address vulnerabilities in Microsoft Windows, Office, Visual Studio, ISA Server, BizTalk Server, Remote Desktop Connection Client for Mac, and .NET Framework as part of the [Microsoft Security Bulletin Summary for August 2009](#). These vulnerabilities may allow an attacker to execute arbitrary code, operate with escalated privileges,

or cause a denial-of-service condition. Additional information regarding these vulnerabilities can be found in US-CERT Technical Cyber Security Alert [TA09-223A](#).

- A public report of a vulnerability affecting the Microsoft Internet Information Services (IIS) FTP service may allow a remote attacker to execute arbitrary code. US-CERT encourages administrators to disable anonymous write access to the FTP server to help mitigate the vulnerability, although a proper impact analysis should be performed prior to taking defensive measures.
- The Mozilla Foundation released Firefox 3.0.13 and Firefox 3.5.2 to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code, display misleading SSL information about a web page, intercept and modify encrypted communication, execute arbitrary JavaScript with chrome privileges, or cause a denial-of-service condition. US-CERT encourages users to review the Mozilla Foundation security advisories for [Firefox 3.0](#) and [Firefox 3.5](#) and apply any necessary updates or workarounds to help mitigate the risks.

### **Technical Cyber Security Alerts**

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

<b>Technical Cyber Security Alerts for August 2009</b>	
<b>August 6</b>	<a href="#">TA09-218A Apple Updates for Multiple Vulnerabilities</a>
<b>August 11</b>	<a href="#">TA09-223A Microsoft Updates for Multiple Vulnerabilities</a>

### **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.

<b>Cyber Security Alerts (non-technical) for August 2009</b>	
<b>August 6</b>	<a href="#">SA09-218A Apple Updates for Multiple Vulnerabilities</a>
<b>August 11</b>	<a href="#">SA09-223A Microsoft Updates for Multiple Vulnerabilities</a>

### **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 (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

<b>Security Bulletins for August 2009</b>
<a href="#">SB09-215 Vulnerability Summary for the Week of July 27, 2009</a>
<a href="#">SB09-222 Vulnerability Summary for the Week of August 3, 2009</a>
<a href="#">SB09-229 Vulnerability Summary for the Week of August 10, 2009</a>
<a href="#">SB09-236 Vulnerability Summary for the Week of August 17, 2009</a>
<a href="#">SB09-243 Vulnerability Summary for the Week of August 24, 2009</a>

A total of 527 vulnerabilities were recorded in the [NVD](#) during August 2009.

## Cyber Security Tips

[Cyber Security Tips](#) are primarily intended for non-technical computer users and are issued monthly. The August tips focused on the benefits of BCC, and identifying hoaxes and urban legends.

<b>Cyber Security Tips for August 2009</b>	
<b>August 13</b>	<a href="#">ST04-008 Benefits of BCC</a>
<b>August 26</b>	<a href="#">ST04-009 Identifying Hoaxes and Urban Legends</a>

## Security Highlights

### GFIRST 2009 National Conference

The Government Forum of Incident Response and Security Teams (GFIRST) hosted the fifth annual GFIRST National Conference in Atlanta, Georgia during August 2009. The conference focused on Threat, Vulnerability, Attack & Detection, Mitigation, and Reflection. These foundations support the cyber security and incident response community by identifying the core components of incident management. Regardless of sector, these five pillars provide a framework to secure information systems.

*Threat* is the collection and analysis of information regarding attacks and/or malware utilized to breach controls in information systems that would otherwise be unavailable to our constituency. Organizations need to understand the threats (identity and intentions), and their capabilities. Understanding the threat assists organizations in prioritizing and protecting systems against them.

*Vulnerability* is the identification and aggregation of exploitable weaknesses in information systems from an authoritative source. Understanding the vulnerabilities being exploited by attackers is a key factor in planning the release of information and protecting systems. Once the vulnerabilities are understood, they can be prioritized against other vulnerabilities to determine which are the most important to protect against and mitigate first (i.e., patching). Prioritization allows organizations to release high quality products with the most important, relevant information.

*Attack & Detection* comprise of actions used to identify threat activity that exists in a complex, multi-agency, multi-platform environment. Attack & Detection is better implemented once an organization understands the threat and the vulnerabilities being exploited. After this information is understood, organizations can implement the appropriate detection mechanisms on their systems.

*Mitigation* involves solutions that contain or resolve risks through analysis of threat activity and vulnerability data. Mitigation should provide timely and accurate responses for organizations to

prevent attacks, reduce vulnerabilities, and fix systems. Mitigation can be difficult and time consuming to implement. However, an effective mitigation strategy should be formed based on an understanding of threats, vulnerabilities, and their prioritization.

*Reflection* is used to mature and develop the defenses of critical information systems by compelling or influencing changes in law, regulation, policy, or procedure. Reflection allows organizations to review the threats, vulnerabilities exploited, attacks and overall system posture to implement policy and technology changes that will assist in protecting systems from similar incidents in the future.

## **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](mailto:info@us-cert.gov).

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

Email Address: [info@us-cert.gov](mailto: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>