



# US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

## Monthly Activity Summary - November 2009 -

This report summarizes general activity as well as updates made to the [National Cyber Alert System](#) for November 2009. It 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 November 2009, US-CERT issued 11 Current Activity entries, one (1) Technical Cyber Security Alert, one (1) Cyber Security Alert, five (5) weekly Cyber Security Bulletins, and two (2) Cyber Security Tips.

Highlights for this month include updates released by Adobe, Apple, Microsoft, Research in Motion (RIM) BlackBerry, and Sun; a Secure Sockets Layer (SSL) and Transport Layer Security (TLS) vulnerability; and phishing messages impersonating the Social Security Administration.

### 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>3</b>
<b>Security Highlights.....</b>	<b>4</b>
<b>Contacting US-CERT.....</b>	<b>4</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 November 2009</b>	
<b>November 4</b>	<a href="#">Sun Releases Update 17 for Java SE 6</a>
<b>November 4</b>	<a href="#">Adobe Releases Update for Shockwave Player</a>
<b>November 5</b>	<a href="#">Microsoft Releases Advance Notification for November Security Bulletin</a>
<b>November 5</b>	<a href="#">BlackBerry Desktop Manager Vulnerability</a>
<b>November 10</b>	<a href="#">Microsoft Releases November Security Bulletin</a>
<b>November 10</b>	<a href="#">Apple Releases Mac OS X v10.6.2 and Security Update 2009-006</a>

<b>Current Activity for November 2009</b>	
<b>November 12</b>	<a href="#">Apple Releases Safari 4.0.4</a>
<b>November 16</b>	<a href="#">Microsoft Releases Security Advisory 977544</a>
<b>November 16</b>	<a href="#">SSL and TLS Vulnerable to Man-in-the-middle Attacks</a>
<b>November 23</b>	<a href="#">Microsoft Releases Security Advisory 977981</a>
<b>November 24</b>	<a href="#">Malicious Code Circulating via Social Security Administration Phishing Messages</a>

- Adobe released Shockwave Player 11.5.2.602 to address multiple vulnerabilities. Exploitation of these vulnerabilities may allow an attacker to run malicious code on the user's machine. US-CERT encourages users and administrators to review Adobe security bulletin [APSB09-16](#) and update to Shockwave Player 11.5.2.602 to help mitigate the risks.
- Apple released security updates for Mac OS X and Safari in November:
  - Mac OS X v10.6.2 and Security Update [2009-006](#) addressed multiple vulnerabilities in a number of applications. These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, conduct a man-in-the-middle attack, operate with escalated privileges, or obtain sensitive information.
  - Safari 4.0.4 addressed multiple vulnerabilities in a number of components. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, conduct cross-site request forgery, or obtain sensitive information. These vulnerabilities affect Safari running on both the Mac OS X and Windows platforms. Refer to Apple article [HT3949](#) for additional details.
- Microsoft released its monthly security bulletin and two advisories in November:
  - Microsoft's Security Bulletin for [November 2009](#) contained six bulletins, including three rated Critical and three rated Important. The bulletins affected Windows and Microsoft Office. These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, or operate with escalated privileges. Additional details are also described in Technical Cyber Security Alert [TA09-342A](#).
  - Microsoft released security advisory [977544](#) to address a vulnerability in the Server Message Block (SMB) protocol. This vulnerability may allow an attacker to cause a denial-of-service condition. This vulnerability only affects Windows 7 and Server 2008 software.
  - Microsoft released security advisory [977981](#) to address a vulnerability in Microsoft Internet Explorer. This vulnerability may allow an attacker to execute arbitrary code.
- RIM released Security Advisory [KB19701](#) to address a vulnerability in BlackBerry Desktop Manager that may allow an attacker to execute arbitrary code. According to the bulletin, "a malicious user may be able to deceive a legitimate user into connecting to a web site that is controlled by the malicious user to allow remote code execution on the legitimate user's computer."
- Sun released update 17 for Java SE JDK 6 and Java SE JRE 6 to address multiple vulnerabilities. The impacts of these vulnerabilities include arbitrary code execution, privilege escalation, denial of service, and information disclosure. Additional details can be found in the Java SE 6 Update 17 [release notes](#).

## 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 November 2009</i>	
<b>November 10</b>	<a href="#">TA09-314A 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.

<i>Cyber Security Alerts (non-technical) for November 2009</i>	
<b>November 10</b>	<a href="#">SA09-314A 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 (NCSA) / US-CERT. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

<i>Security Bulletins for November 2009</i>	
	<a href="#">SB09-306 Vulnerability Summary for the Week of October 26, 2009</a>
	<a href="#">SB09-313 Vulnerability Summary for the Week of November 2, 2009</a>
	<a href="#">SB09-320 Vulnerability Summary for the Week of November 9, 2009</a>
	<a href="#">SB09-327 Vulnerability Summary for the Week of November 16, 2009</a>
	<a href="#">SB09-334 Vulnerability Summary for the Week of November 23, 2009</a>

A total of 314 vulnerabilities were recorded in the [NVD](#) during November 2009.

## Cyber Security Tips

[Cyber Security Tips](#) are primarily intended for non-technical computer users. The November tips focused on denial-of-service attacks and spyware.

<i>Cyber Security Tips for November 2009</i>	
<b>November 4</b>	<a href="#">ST04-015 Understanding Denial-of-Service Attacks</a>
<b>November 19</b>	<a href="#">ST04-016 Recognizing and Avoiding Spyware</a>

## ***Security Highlights***

### **SSL and TLS Vulnerable to Man-in-the-Middle Attacks**

US-CERT became aware of reports of publicly available exploit code for a vulnerability within the SSL and TLS protocols. Reports indicated that exploitation of this vulnerability potentially allowed an attacker to conduct a man-in-the-middle attack, allowing an attacker to inject plaintext into the beginning of the application protocol stream.

US-CERT encouraged OpenSSL users and administrators to review the [OpenSSL 0.9.8i](#) release and apply any updates.

### **Malicious Code Circulating via Social Security Administration Phishing Messages**

US-CERT became aware of public reports of malicious code circulating via phishing email messages that appear to come from the Social Security Administration. The messages indicated that the users' annual Social Security statements may contain errors and instructed users to follow a link to review their Social Security statement. If users clicked this link, they were redirected to a seemingly legitimate website that prompted them for their Social Security number. If users entered their Social Security number and continued to the next page, they were given an option to generate a statement. If users attempted to generate a statement, malicious code could have been installed on their systems. This malicious code attempted to collect online banking traffic to gain access to the users' bank accounts.

US-CERT encouraged users and administrators to take the following preventative measures to help mitigate the security risks:

- Install antivirus software, and keep the virus signatures up to date.
- Do not follow unsolicited links, and do not open unsolicited email messages.
- Use caution when visiting untrusted websites.
- Use caution when entering personal information online.
- 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](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: [0xCB0CBD6E](#)

PGP Key Fingerprint: 2A10 30D4 3083 2D28 032F 6DE3 3D60 3D81 CB0C BD6E

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