



# US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

## Monthly Activity Summary - October 2009 -

This report summarizes general activity as well as updates made to the [National Cyber Alert System](#) for October 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 October 2009, US-CERT issued 11 Current Activity entries, three (3) Technical Cyber Security Alerts, two (2) Cyber Security Alerts, four (4) weekly Cyber Security Bulletins, and two (2) Cyber Security Tips.

Highlights for this month include updates released by Research in Motion, Microsoft, Adobe, Oracle, and Mozilla.

### 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 October 2009</b>	
<b>October 1</b>	<a href="#">Research in Motion Releases Security Advisory</a>
<b>October 6</b>	<a href="#">Federal Bureau of Investigation Warns Public of Fraudulent Spam Email</a>
<b>October 8</b>	<a href="#">Microsoft Releases Advance Notification for October Security Bulletin</a>
<b>October 8</b>	<a href="#">Adobe Releases Security Bulletin for Critical Vulnerability</a>
<b>October 13</b>	<a href="#">Adobe Releases Security Bulletin for Adobe Reader and Acrobat</a>
<b>October 13</b>	<a href="#">Microsoft Releases October Security Bulletin</a>
<b>October 15</b>	<a href="#">Malware Spam Messages Related to Microsoft Outlook, SSL Certificates</a>
<b>October 20</b>	<a href="#">Oracle Releases Critical Patch Update for October 2009</a>

<b>Current Activity for October 2009</b>	
<b>October 27</b>	<a href="#">BlackBerry PhoneSnoop Application Used to Spy on Users</a>
<b>October 27</b>	<a href="#">Federal Deposit Insurance Corporation Warns Public of Fraudulent Email</a>
<b>October 28</b>	<a href="#">Mozilla Releases Firefox 3.0.15 and Firefox 3.5.4</a>

- Research in Motion has released a [security advisory](#) to address a vulnerability related to how null characters are displayed in a BlackBerry dialog box. This vulnerability may allow an attacker to trick users into believing that they are connecting to a trusted secure site. US-CERT encourages users to review the BlackBerry security advisory [KB19552](#) and apply any necessary [updates](#).
  - BlackBerry devices were also impacted by a new software application called PhoneSnoop. This software allows an attacker to call a user's BlackBerry and listen to personal conversations. In order to install and setup the PhoneSnoop application, attackers must have physical access to the user's device or convince a user to install PhoneSnoop. US-CERT encourages users to only download BlackBerry applications from trusted sources and to password protect and lock BlackBerry devices.
- Microsoft released an update to address vulnerabilities in Microsoft Windows, Silverlight, Internet Explorer, .NET Framework, Office, SQL Server, Developer Tools, and Forefront as part of the Microsoft Security Bulletin Summary for [October 2009](#). These vulnerabilities may allow an attacker to execute arbitrary code, operate with escalated privileges, cause a denial-of-service condition, or spoof an end user or website. Review the [bulletins](#) and refer to Technical Cyber Security Alert [TA09-286A](#) for additional information.
- Adobe released security bulletin [APSB09-15](#) to alert users of a critical vulnerability in Adobe Reader and Acrobat. Adobe indicates that it has received reports of active exploitation of this vulnerability. Release of an update for this vulnerability is scheduled for Tuesday, October 13. Adobe republished security bulletin [APSB09-015](#) to address multiple vulnerabilities in Adobe Reader and Acrobat. These vulnerabilities may allow an attacker to execute arbitrary code, escalate local privileges, or cause a denial-of-service condition. Additional information can be found in Technical Cyber Security Alert [TA09-286B](#).
- Oracle released its [Critical Patch Update for October 2009](#) to address 38 vulnerabilities across several products. This update contains security fixes for the Oracle Database; Oracle Application Server; Oracle E-Business Suite and Applications; Oracle PeopleSoft and JD Edwards Suite; Oracle BEA Products Suite; and Oracle Industry Applications Products Suite. Additional information is available in Technical Cyber Security Alert [TA09-294A](#).
- Mozilla released Firefox 3.0.15 and Firefox 3.5.4 to address multiple vulnerabilities. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code, execute arbitrary JavaScript with chrome privileges, or cause a denial-of-service condition. As described in the Mozilla Foundation Security Advisories, some of these vulnerabilities may also affect SeaMonkey. Refer to Mozilla Foundation security advisories for [Firefox 3.0](#) and [Firefox 3.5](#) for additional information.

## 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 October 2009</i>	
<b>October 8</b>	<a href="#">TA09-286A Microsoft Updates for Multiple Vulnerabilities</a>
<b>October 13</b>	<a href="#">TA09-286B Adobe Reader and Acrobat Vulnerabilities</a>
<b>October 13</b>	<a href="#">TA09-294A Oracle 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 October 2009</i>	
<b>October 13</b>	<a href="#">SA09-286A Microsoft Updates for Multiple Vulnerabilities</a>
<b>October 13</b>	<a href="#">SA09-286B Adobe Reader and Acrobat 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) / 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 October 2009</i>	
	<a href="#">SB09-278 Vulnerability Summary for the Week of September 28, 2009</a>
	<a href="#">SB09-285 Vulnerability Summary for the Week of October 5, 2009</a>
	<a href="#">SB09-292 Vulnerability Summary for the Week of October 12, 2009</a>
	<a href="#">SB09-299 Vulnerability Summary for the Week of October 19, 2009</a>

A total of 353 vulnerabilities were recorded in the [NVD](#) during October 2009.

## Cyber Security Tips

[Cyber Security Tips](#) are primarily intended for non-technical computer users and are issued monthly. The October tips focused on privacy, and avoiding social engineering/phishing attacks.

<i>Cyber Security Tips for October 2009</i>	
<b>October 8</b>	<a href="#">ST04-013 Protecting Your Privacy</a>
<b>October 22</b>	<a href="#">ST04-014 Avoiding Social Engineering and Phishing Attacks</a>

## **Security Highlights**

### ***Malware Spam Messages Related to Microsoft Outlook, SSL Certificates***

Public reports circulated regarding an increase in the number of spam messages related to Microsoft Outlook or SSL certificates. These messages contain a malicious file or link that claims to provide an update, but in reality, attempts to launch malware on a user's system. Typically, the messages instruct the user to click on a link to save a file or to open an attachment, either of which could infect the user's system.

### ***Federal Bureau of Investigation Warns Public of Fraudulent Spam Email***

The Federal Bureau of Investigation (FBI) has released information warning the public about fraudulent email messages purporting to come from the FBI or the Department of Homeland Security. These email messages contain a malicious attachment that claims to provide an intelligence report or bulletin, but in reality attempts to launch malware on the user's system.

More information regarding these messages can be found in the [Federal Bureau of Investigation's New E-Scams and Warnings](#) web site.

### ***Federal Deposit Insurance Corporation Warns Public of Fraudulent Email***

The Federal Deposit Insurance Corporation (FDIC) has released information warning the public about fraudulent email messages purporting to come from the FDIC. These email messages provides a link to a fraudulent FDIC website. Users are then instructed to download their "personal FDIC Insurance File." More information regarding these messages can be found in the [Federal Deposit Insurance Corporation's Consumer Alerts](#) website.

To help protect against this type of attack, US-CERT recommends that users avoid opening attachments contained in unsolicited email messages. To help protect against this type of attack, US-CERT recommends that users avoid opening attachments or links contained in unsolicited email messages. Additional tips regarding email attachments can be found in the US-CERT Cyber Security Tip [Using Caution with Email Attachments](#).

## **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>