



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary - May 2011 -

This report summarizes general activity including updates to the [National Cyber Alert System](#) in May 2011. 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 May 2011, US-CERT issued 14 Current Activity entries, one Technical Cyber Security Alert, one Cyber Security Alert, five weekly Cyber Security Bulletins, and two Cyber Security Tips.

Highlights for this month include updates or advisories released by Microsoft, Apple, Adobe, the Internet System Consortium, Google, and Cisco.

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 reported to US-CERT. The table lists all of the entries posted this month followed by a brief overview of the most significant entries.

Current Activity for May 2011	
May 2	Osama Bin Laden's Death E-mail Scams, Fake Antivirus, and Phishing Attack Warning
May 5	Microsoft Releases Advance Notification for May Security Bulletin
May 9	Apple Releases iOS 4.3.3
May 10	Microsoft Releases May Security Bulletin
May 13	Google Releases Chrome 11.0.696.68
May 13	Adobe Releases Flash Player and Flash Media Server Updates
May 16	Mississippi Flooding Disaster E-mail Scams, Fake Antivirus, and Phishing Attack Warning
May 16	WebGL Security Risks
May 19	Microsoft Releases New Version of EMET

Current Activity for May 2011	
May 25	Google Chrome Releases 11.0.696.71
May 25	Apple Mac Defender, MacProtector, and MacSecurity Fake Anti-Virus Software
May 26	Cisco Releases Security Advisory for Cisco Internet Streamer
May 26	WordPress Releases Version 3.1.3
May 27	Internet System Consortium releases BIND patches

- The [Microsoft Security Bulletin Summary for May 2011](#) provided updates to address vulnerabilities in Microsoft Windows and Microsoft Office. These vulnerabilities may allow an attacker to execute arbitrary code.
- Apple released an update for iOS and a security advisory:
 - [iOS 4.3.3 Software Update](#) addressed two bugs in iOS that resulted in the devices storing historical location data for too long.
 - Apple article [HT4650](#) provided tips for users on how to avoid or remove the MacDefender fake antivirus (AV) software. This fake anti-virus software is the result of a phishing scam targeting Mac users that redirects them from legitimate websites to fake websites. The ultimate goal of the fake anti-virus software is to steal the user's credit card information.
- Adobe released updates for Flash Player and Flash Media Server to address multiple vulnerabilities. These vulnerabilities affect Adobe Flash Player 10.2.159.1 and earlier versions for Windows, Macintosh, Linux, and Solaris; Adobe Flash Player 10.2.157.51 and earlier versions for Android; Adobe Flash Media Server 4.0.1 and earlier versions; and Adobe Flash Media Server 3.5.5 and earlier versions for Windows and Linux. Exploitation of these vulnerabilities may allow an attacker to cause a denial-of-service condition or execute arbitrary code. US-CERT encourages users and administrators to review Adobe Security Advisories [APSB11-11](#) and [APSB11-12](#) and apply any necessary updates to help mitigate the risks.
- The Internet System Consortium released updates for BIND to address a vulnerability in BIND versions 9.4-ESV-R3 and later, 9.6-ESV-R2 and later, 9.6.3, 9.7.1 and later, and 9.8.0 and later. Exploitation of this vulnerability may allow an attacker to cause a denial-of-service condition. Additional information regarding this vulnerability is located in the US-CERT Vulnerability Note [VU#795694](#). US-CERT encourages users and administrators to review [CVE-2011-1910](#) and apply the respective patches to help mitigate the risks. Since BIND is packaged in larger third-party applications or operating system distributions, users and administrators should check with their software vendors for updated versions.
- Google released two updates for the Chrome Web browser in May 2011. The updates addressed vulnerabilities that enabled attackers to execute arbitrary code. The latest version released was Chrome 11.0.696.71.
- Cisco released a security advisory to address a vulnerability in the web server component of the Cisco Internet Streamer application, which is part of the Cisco Content Delivery System. This vulnerability may allow an attacker to cause a denial-of-service condition. US-CERT encourages users and administrators to review Cisco security advisory [cisco-sa-20110525-spcdn](#) and apply any necessary updates or workarounds to help mitigate the risks.

Technical Cyber Security Alerts

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

<i>Technical Cyber Security Alerts for May 2011</i>	
<i>May 10</i>	TA11-130A Microsoft Updates for Multiple Vulnerabilities

Cyber Security Alerts

[Cyber Security Alerts](#) 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 May 2011</i>	
<i>May 10</i>	SA11-130A Microsoft Updates for Multiple 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's (NIST's) [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>Cyber Security Bulletins for May 2011</i>	
<i>May 2</i>	SB11-122 Vulnerability Summary for the Week of April 25, 2011
<i>May 9</i>	SB11-129 Vulnerability Summary for the Week of May 2, 2011
<i>May 16</i>	SB11-136 Vulnerability Summary for the Week of May 9, 2011
<i>May 23</i>	SB11-143 Vulnerability Summary for the Week of May 16, 2011
<i>May 31</i>	SB11-150 Vulnerability Summary for the Week of May 23, 2011

A total of 295 vulnerabilities were recorded in the NVD during May 2011.

Cyber Security Tips

[Cyber Security Tips](#) are primarily intended for non-technical computer users. The focus of May's tips was keeping children safe online.

<i>Cyber Security Tips for May 2011</i>	
<i>May 18</i>	ST05-002 Keeping Children Safe Online
<i>May 18</i>	ST06-005 Dealing with Cyberbullies

Security Highlights

Mississippi Flooding Disaster E-mail Scams, Fake Antivirus, and Phishing Attack Warning

Users should be aware of potential e-mail scams, fake antivirus, and phishing attacks regarding the Mississippi flooding disaster. E-mail scams may contain links or attachments that may direct users to phishing or malicious websites. Fake antivirus attacks may come in the form of pop-ups that flash security warnings and ask the user for credit card information. Phishing e-mails and websites requesting donations for bogus charitable organizations commonly appear after these types of natural disasters.

US-CERT encourages users to take the following measures to protect themselves:

- Do not follow or open unsolicited web links or attachments in e-mail messages. Maintain up-to-date antivirus software.
- Review the [Recognizing Fake Antivirus](#) document for additional information on recognizing fake antivirus.
- Refer to the [Avoiding Social Engineering and Phishing Attacks](#) document for additional information on social engineering attacks.
- Refer to the [Recognizing and Avoiding E-mail Scams](#) (pdf) document for additional information on avoiding e-mail scams.
- Review the Federal Trade Commission's [Charity Checklist](#).
- Verify the legitimacy of the e-mail by contacting the organization directly through a trusted contact number. Information related to trusted contact is located on the Better Business Bureau [National Charity Report Index](#).

Contacting US-CERT

If you would like to contact US-CERT to ask a question, submit an incident, or 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 e-mail info@us-cert.gov.

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

E-mail Address: info@us-cert.gov

Phone Number: +1 (888) 282-0870

PGP Key ID: [0x91D70D64](#)

PGP Key Fingerprint: EAAC 46A4 4CEC 8A78 EED2 73F3 E5F3 5D6C 91D7 0D64

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