



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary - March 2011 -

This report summarizes general activity including updates to the [National Cyber Alert System](#) in March 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 March 2011, US-CERT issued 23 Current Activity entries, one Technical Cyber Security Alert, one Cyber Security Alert, four weekly Cyber Security Bulletins, and one Cyber Security Tip.

Highlights for this month include updates or advisories released by Adobe, Apple, Google, Microsoft, and multiple phishing attacks.

Contents

Executive Summary	1
Current Activity	1
Technical Cyber Security Alerts	3
Cyber Security Alerts	3
Cyber Security Bulletins	4
Cyber Security Tips	4
Security Highlights	4
Contacting US-CERT	6

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 March 2011	
March 1	Google Releases Chrome 9.0.597.107
March 2	Mozilla Releases Updates for Firefox, Thunderbird, and SeaMonkey
March 3	Apple Releases iTunes 10.2
March 8	Microsoft Releases March Security Bulletin
March 8	Microsoft Releases Advance Notification for March Security Bulletin
March 9	Apple Releases Java Updates for Mac OS X 10.5 and OS X 10.6
March 9	Google Releases Chrome 10.0.648.127
March 10	Apple Releases Safari 5.0.4
March 10	Apple Releases iOS 4.3
March 14	Japan Earthquake and Tsunami Disaster Email Scams, Fake Antivirus and Phishing Attack Warning

Current Activity for March 2011	
March 14	Google Releases Chrome 10.0.648.133
March 15	Adobe Releases Security Advisory for Flash Player, Reader, and Acrobat
March 16	US Tax Season Phishing Scams and Malware Campaigns
March 16	BlackBerry WebKit Browser Engine Vulnerability
March 17	Google Releases Chrome 10.0.648.134
March 18	Ongoing Phishing Attack
March 22	Adobe Releases Security Updates for Reader and Acrobat
March 22	Apple Releases Security Updates
March 23	Fraudulent SSL Certificates
March 24	Adobe Releases Flash Player Update
March 25	Google Releases Chrome 10.0.648.204
March 25	VideoLAN Releases VLC Media Player 1.1.8
March 31	Cisco Releases Security Advisories

- Google released five updates for the Chrome Web browser in March 2011. The updates addressed vulnerabilities that enabled attackers to execute arbitrary code, cause denial-of-service conditions, bypass security restrictions, and exploit Adobe Flash. The latest version released was [Chrome 10.0.648.204](#).
- Adobe released advisories for Flash Player, Reader, and Acrobat in March 2011. The updates addressed vulnerabilities that might allow an attacker to cause a denial-of-service attack or execute arbitrary code. US-CERT encourages users and administrators to review Adobe Security Advisory [APSB11-05](#) and [APSB11-06](#) and apply any necessary updates to help mitigate the risks.
- Research In Motion has released a security notice to alert users of a vulnerability affecting the WebKit browser engine provided in BlackBerry Device Software versions 6.0 and later. By convincing a user to browse to specially crafted website, a remote attacker may be able to execute arbitrary code. Exploitation of this vulnerability may allow an attacker to access user data stored on the media card and the built-in media storage on the affected BlackBerry device. US-CERT encourages users and administrators to review BlackBerry security notice KB26132 and do the following to help mitigate the risks:
 - Exercise caution when accessing untrusted websites in browsers, email messages, or instant messages.
 - Disable the use of JavaScript in the BlackBerry Browser or Disable the BlackBerry Browser as suggested in BlackBerry security notice [KB26132](#).
- Apple released Mac OS X v10.6.7 and Security Update 2011-001 to address multiple vulnerabilities. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, or obtain sensitive information. US-CERT encourages users and administrators to review Apple article [HT4581](#) and apply any necessary updates to help mitigate the risks.

- US-CERT is aware of public reports of the existence of fraudulent SSL certificates. These fraudulent SSL certificates could be used by an attacker to masquerade as a trusted website. Multiple web browser vendors have provided updates to recognize and block these fraudulent SSL certificates. Mozilla has updated Firefox 4.0, 3.6, and 3.5. Additional information can be found in the [Mozilla Security Blog](#). Microsoft has released updates for various platforms in [Microsoft Knowledge Base Article 2524375](#). Additional information can be found in [Microsoft Security Advisory 2524375](#). US-CERT encourages users and administrators to apply any necessary updates to help mitigate the risks. US-CERT will provide additional information as it becomes available.
- VideoLAN has released VLC Media Player 1.1.8 to address two vulnerabilities. These vulnerabilities are due to the improper handling of .AMV and .NSV files. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code. US-CERT encourages users and administrators to review the [release notes](#) for VLC Media Player 1.1.8 and apply any necessary updates to help mitigate the risks.
- Cisco released a security advisory to address a vulnerability in some versions of Cisco Secure Access Control System (ACS). This vulnerability may allow an attacker to change the password of a user account without any previous access to the user's account or knowledge of the account's previous password. Additionally, Cisco has released a security advisory to address a vulnerability in some versions of the Cisco Network Access Control (NAC) Guest Server System Software. This vulnerability may allow an unauthenticated user to access the protected network. US-CERT encourages users and administrators to review Cisco security advisories [cisco-sa-20110330-acs](#) and [cisco-sa-20110330-nac](#) and apply any necessary updates 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.

<i>Technical Cyber Security Alerts for March 2011</i>	
March 8	TA11-067A Microsoft Updates for Multiple 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 March 2011</i>	
March 8	SA11-067A 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.

Security Bulletins for March 2011	
	SB11-066 Vulnerability Summary for the Week of February 28, 2011
	SB11-073 Vulnerability Summary for the Week of March 7, 2011
	SB11-080 Vulnerability Summary for the Week of March 14, 2011
	SB11-087 Vulnerability Summary for the Week of March 21, 2011

A total of 355 vulnerabilities were recorded in the NVD during March 2011.

Cyber Security Tips

[Cyber Security Tips](#) are primarily intended for non-technical computer users. The focus of March's tip was common computer use and security myths.

Cyber Security Tips for March 2011	
March 9	ST06-006 Understanding Hidden Threats: Corrupted Software Files

Security Highlights

Japan Earthquake and Tsunami Disaster Email Scams, Fake Antivirus, and Phishing Attack Warning

US-CERT would like to warn users of potential email scams, fake antivirus, and phishing attacks regarding the Japan earthquake and the tsunami disasters. Email scams may contain links or attachments which may direct users to phishing or malware-laden 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 that request donations for bogus for 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 unsolicited web links or attachments in email 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 Email Scams](#) (pdf) document for additional information on avoiding email scams.
- Review the Federal Trade Commission's [Charity Checklist](#).
- Verify the legitimacy of the email by contacting the organization directly through a trusted contact number. Trusted contact information is listed on the Better Business Bureau [National Charity Report Index](#).

US-CERT will provide additional information as it becomes available.

US Tax Season Phishing Scams and Malware Campaigns

In the past, US-CERT has received reports of an increased number of phishing scams and malware campaigns that take advantage of the United States tax season. Due to the upcoming tax deadline, US-CERT reminds users to remain cautious when receiving unsolicited email that could be part of a potential phishing scam or malware campaign.

These phishing scams and malware campaigns may include, but are not limited to, the following:

- information that refers to a tax refund
- warnings about unreported or under-reported income
- offers to assist in filing for a refund
- details about fake e-file websites

These messages, which may appear to be from the IRS, may ask users to submit personal information via email or may instruct the user to follow a link to a website that requests personal information or contains malicious code.

US-CERT encourages users and administrators to take the following measures to protect themselves from these types of phishing scams and malware campaigns:

- Do not follow unsolicited web links in email messages.
- Maintain up-to-date antivirus software.
- Refer to the [IRS website](#) related to phishing, email, and bogus website scams for scam samples and reporting information.
- 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.
- Review the Wall Street Journal blog post "[Cybercrooks Digging for Tax Data](#)" for additional suggestions for protecting against these types of attacks.

Ongoing Phishing Attack

US-CERT is aware of public reports of an ongoing phishing attack. At this time, this attack appears to be targeting PayPal, Bank of America, Lloyds, and TSB users. The attack arrives via an unsolicited email message containing an HTML attachment.

This attack is unlike common phishing attacks because it locally stores the malicious webpage rather than directing users to a phishing site via a URL. Many browsers utilize anti-phishing filters to help protect users against phishing attacks; this method of attack is able to bypass this security mechanism.

US-CERT encourages users and administrators to take the following measures to protect themselves from these types of phishing attacks:

- Do not follow unsolicited web links or attachments in email messages.
- Use caution when providing personal information online.
- Verify the legitimacy of the email by contacting the organization directly through a trusted contact method.
- 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.
- Refer to the [Using Caution with Email Attachments](#) Cyber Security Tip for more information on safely handling email attachments.

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>