US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary

- February 2012 -

This report summarizes general activity including updates to the National Cyber Awareness System in February 2012. It includes current activity updates, alerts, and bulletins, in addition to other newsworthy events or highlights.

Executive Summary

During February 2012, US-CERT issued 14 Current Activity entries, one Alert, and four weekly Bulletins.

Highlights for this month include updates or advisories released by Microsoft, Adobe, Oracle, Google, and Symantec, as well as a phishing and malware campaign using spoofed US-CERT email addresses.

Contents

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 February 2012	
February 1	Mozilla Releases Firefox 10 and 3.6.26
February 2	Apple Releases Multiple Security Updates
February 8	U.S. Tax Season Phishing Scams and Malware Campaigns
February 8	Google Releases Chrome 17.0.963.46
February 9	Microsoft Releases Advance Notification for February Security Bulletin
February 13	Mozilla Releases Firefox 10.0.1
February 14	Adobe Releases Security Bulletins for Adobe Shockwave Player and RoboHelp
February 14	Microsoft Releases February Security Bulletin
February 14	Oracle Releases Critical Patch Update for February 2012
February 15	Cisco Releases Security Advisory for Cisco NX-OS
February 16	Google Releases Chrome 17.0.963.56
February 16	Adobe Releases Security Advisory for Adobe Flash Player

Current Activity for February 2012	
February 23	DNSChanger Malware
February 29	Cisco Releases Multiple Security Advisories

- Microsoft released updates to address vulnerabilities in Microsoft Windows, Internet Explorer, .Net Framework, Silverlight, Office, and Server Software as part of the Microsoft Security Bulletin Summary for February 2012. These vulnerabilities may allow an attacker to execute arbitrary code or operate with elevated privileges.

- Adobe released three Security Advisories to address vulnerabilities affecting Adobe Shockwave Player, Adobe RoboHelp, and Adobe Flash Player. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, take control of the affected system, or perform a cross-site scripting attack. Affected software versions include the following:
    - Adobe Shockwave Player 11.6.3.633 and earlier versions for Windows and Macintosh
    - Adobe RoboHelp 9 or 8 for Word on Windows
    - Adobe Flash Player 11.1.102.55 and earlier versions for Windows, Macintosh, Linux, and Solaris operating systems
    - Adobe Flash Player 11.1.112.61 and earlier versions for Android 4.x
    - Adobe Flash Player 11.1.111.5 and earlier versions for Android 3.x and 2.x

- Oracle released its Oracle Java SE Critical Patch Update for February 2012 containing 14 security fixes for the following products:
    - JDK and JRE 7 Update 2 and earlier
    - JDK and JRE 5 Update 30 and earlier
    - JDK and JRE 5.0 Update 33 and earlier
    - SDK and JRE 1.4.2_35 and earlier
    - JavaFX 2.0.2 and earlier

- Google released Chrome 17.0.963.46 and Chrome 17.0.963.56 for Linux, Mac, Windows, and Chrome Frame to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition.

- The Mozilla Foundation released Firefox 10.0.1 to address a vulnerability that may cause a denial-of-service condition or potentially allow an attacker to execute arbitrary code.

Alerts

Alerts provide timely information about current security issues, vulnerabilities, and exploits.

Alerts for February 2012	
February 14	TA12-045A Microsoft Updates for Multiple Vulnerabilities

Bulletins

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 (NCSD)/US-CERT. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

Bulletins for February 2012	
February 6	SB12-037 Vulnerability Summary for the Week of January 30, 2012
February 13	SB12-044 Vulnerability Summary for the Week of February 6, 2012
February 20	SB12-051 Vulnerability Summary for the Week of February 13, 2012
February 29	SB12-058 Vulnerability Summary for the Week of February 20, 2012

A total of 353 vulnerabilities were recorded in the NVD during February 2012.

Security Highlights

U.S. 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:

- information that refers to a tax refund,
- warnings about unreported or under-reported income,
- offers to assist in filing for a refund, and
- 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.
- Forward suspected phishing emails to phishing@irs.gov.

Contacting US-CERT

If you would like to contact US-CERT to ask a question, submit an incident, or learn more about cybersecurity, 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.

Web Site Address: http://www.us-cert.gov
E-mail Address: info@us-cert.gov
Phone Number: +1 (703) 235-5110
PGP Key ID: 0xEDA10949
PGP Key Fingerprint: 6040 50FC 1BA3 81FA 0919 1378 C036 EDA1 0949
PGP Key: https://www.us-cert.gov/pgp/info.asc