US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary

- December 2011 -

This report summarizes general activity including updates to the National Cyber Alert System in December 2011. It includes current activity updates, technical and non-technical cyber security alerts, and cyber security bulletins, in addition to other newsworthy events or highlights.

Executive Summary

During December 2011, US-CERT issued 13 Current Activity entries, 2 Technical Cyber Security Alerts, 2 Cyber Security Alerts, 4 weekly Cyber Security Bulletins, and 1 Cyber Security Tip.

Highlights for this month include updates or advisories released by Microsoft, Adobe, Google, and The Mozilla Foundation, as well as a phishing scam and malware campaign directed at USAA members.

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 December 2011	
December 1	Adobe Releases Security Advisory for Adobe Flex SDK
December 2	Holiday Season Phishing Scams and Malware Campaigns
December 6	Adobe Releases Updates for Adobe Reader and Acrobat
December 8	Microsoft Releases Advance Notification for December Security Bulletin
December 8	Adobe Releases Security Advisory for Adobe Reader and Acrobat
December 13	Google Releases Chrome 16.0.912.63
December 13	Microsoft Releases December Security Bulletin
December 15	Microsoft Releases Security Advisory for Vulnerability in TrueType Font Parsing
December 16	Adobe Releases Security Advisory for Adobe Reader and Acrobat
December 19	Personal Device Security During the Holiday Season

Current Activity for December 2011	
December 20	USAA Phishing Scam and Malware Campaign
December 21	Mozilla Releases Firefox 9 and 3.6.25
December 29	Multiple Programming Language Implementations Vulnerable to Hash Table Collision Attacks

- Microsoft released updates to address vulnerabilities in Microsoft Windows, Microsoft Office, and Internet Explorer as part of the Microsoft Security Bulletin Summary for December 2011. These vulnerabilities may allow an attacker to execute arbitrary code or operate with elevated privileges. US-CERT encourages users and administrators to review the bulletin and follow best-practice security policies to determine which updates should be applied.

- Adobe released Security Bulletins ASPA11-04 and APSB11-30 to address a vulnerability affecting Adobe Reader and Adobe Acrobat. Exploitation of this vulnerability may allow an attacker to cause a denial-of-service condition or take control of the affected system. US-CERT encourages users and administrators to review the Adobe Security Bulletins for additional information. Affected software versions include:
  - Adobe Reader X (10.1.1) and earlier versions for Windows and Macintosh
  - Adobe Reader 9.4.6 and earlier 9.x versions for Windows, Macintosh, and Unix
  - Adobe Acrobat X (10.1.1) and earlier 10.x versions for Windows and Macintosh
  - Adobe Acrobat 9.4.6 and earlier 9.x versions for Windows and Macintosh
- Adobe released a security advisory to alert users of a vulnerability affecting Adobe Flex SDK 4.5.1 and earlier 4.X versions and Adobe Flex SDK 3.6 and earlier 3.X versions for Windows, Macintosh, and Linux operating systems. Exploitation of this vulnerability may allow an attacker to perform a cross-site scripting attack within the Adobe Flex SDK application.
- Google released Chrome 16.0.912.63 for Linux, Mac, Windows, and Chrome Frame to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code.
- The Mozilla Foundation released Firefox 9 and Firefox 3.6.25 to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, or perform a cross-site scripting attack.

Technical Cyber Security Alerts

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

Technical Cyber Security Alerts for December 2011	
December 13	TA11-347A Microsoft Updates for Multiple Vulnerabilities
December 16	TA11-350A Adobe 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.

Cyber Security Alerts (non-technical) for December 2011	
December 13	SA11-347A Microsoft Updates for Multiple Vulnerabilities
December 16	SA11-350A Adobe 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 (NIST) 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.

Cyber Security Bulletins for December 2011	
December 5	SB11-339 Vulnerability Summary for the Week of November 28, 2011
December 12	SB11-346 Vulnerability Summary for the Week of December 5, 2011
December 19	SB11-353 Vulnerability Summary for the Week of December 12, 2011
December 27	SB11-360 Vulnerability Summary for the Week of December 19, 2011

A total of 337 vulnerabilities were recorded in the NVD during December 2011.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users. The focus of December's tip was Internet Service Providers (ISPs).

Cyber Security Tips for December 2011	
December 19	ST11-001 Holiday Traveling with Personal Internet-Enabled Devices

Security Highlights

USAA Phishing Scam and Malware Campaign

US-CERT is aware of public reports of an active spear-phishing attack via email messages directed at United Services Automobile Association (USAA) members. These messages contain the subject line “Deposit Posted” and contain a randomly generated four-digit number placed in the USAA security zone section. The messages ask users to open an attached file containing malicious software that if activated could provide access to a user's personal information.

US-CERT encourages users to do the following to help mitigate the risk:

- Review the alert posted by USAA regarding this issue.
- Do not open attachments in email messages from unknown sources.
- 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.
- Install anti-virus software and keep virus signature files up to date.

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: 0xEDA10949
PGP Key Fingerprint: 6040 50FC 1BA3 81FA 0919 1378 C036 EDA1 0949
PGP Key: https://www.us-cert.gov/pgp/info.asc