US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary

- September 2008 -

This report summarizes general activity as well as updates made to the National Cyber Alert System for the month of September. 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 the month of September 2008, US-CERT issued 29 Current Activity entries, two (2) Technical Cyber Security Alerts, two (2) Cyber Security Alerts, five (5) weekly Cyber Security Bulletins, and two (2) Cyber Security Tips.

Highlights for this month include multiple web browsers affected by Clickjacking, phishing scams, and multiple updates released by VMware, Microsoft, Google, Apple, Adobe, Mozilla, 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………………….………….4

Security Highlights………………….…………...4

Contacting US-CERT…………………………...5

Current Activity

Current Activity entries are high-impact types of security incidents currently being reported to US-CERT. This month's highlights and activity are listed below.

- VMware released security announcements regarding multiple vulnerabilities in VMware Workstation, Player, ACE, Server, and ESX. These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, access the system with elevated privileges, or obtain sensitive information. VMware also released updates for the ESXi and ESX 3.5 packages to address buffer overflow vulnerabilities in "openwsman."
- Microsoft's September security bulletin provided critical updates for Microsoft Windows, Internet Explorer, .NET Framework, Office, SQL Server, and Visual Studio.
- US-CERT received reports of several vulnerabilities affecting Google's Chrome web browser, including buffer overflow conditions, an out of bounds memory error, and a default configuration allowing downloads to the desktop without prompting the user. Google released Chrome version 0.2.149.29 to address these vulnerabilities.
- Apple released multiple updates to address vulnerabilities in Java for Mac OS X 10.4 and 10.5, Mac OS X, and related products: iTunes, QuickTime, iPod, Bonjour for Windows, and iPhone.

- Adobe released a Security Advisory to alert users of potential vulnerabilities affecting the Macintosh version of Illustrator CS2. By convincing a user to open a malicious Adobe Illustrator file, an attacker may be able to execute arbitrary code. Additionally, US-CERT received public reports of improved attack toolkits for exploiting vulnerabilities in Adobe PDF Reader.
- Mozilla released Firefox versions 3.0.2, 3.0.3, and Thunderbird version 2.0.0.17 to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code, obtain sensitive information, conduct cross-site scripting attacks, cause a denial-of-service condition, operate with escalated privileges, or conduct Clickjacking attacks.
- Cisco released a Security Advisory and a Security Response to address multiple vulnerabilities in Cisco PIX, ASA and Cisco Secure ACS. These vulnerabilities may allow an attacker to cause a denial-of-service condition or obtain sensitive information. Additionally, Cisco released multiple Security Alerts to address vulnerabilities in the Unified Communications Manager and IOS that may allow a remote, unauthenticated attacker to cause a denial-of-service condition, obtain sensitive information, or operate with escalated privileges.

Current Activity for September 2008	
September 1	Hurricane Gustav and Phishing Scams
September 2	VMware Releases Security Announcement
September 3	Google Chrome Download Vulnerability
September 4	Microsoft Releases Advance Notification for September Security Bulletin
September 4	FCC Releases Public Notice about Phishing Scam
September 4	Novell Releases Update for iPrint Vulnerability
September 5	Cisco Releases Advisory and Security Response
September 8	Exploit Code Available for CitectSCADA Vulnerability
September 9	Microsoft Releases September Security Bulletin
September 9	Google Releases Chrome Version 0.2.149.29
September 9	WordPress Releases Version 2.6.2
September 10	U.S. Presidential Election and Phishing Scams
September 10	Apple Releases Security Updates
September 11	DHS Email Scam
September 12	TWiki Releases Security Alert
September 12	Apple Releases iPhone v2.1
September 15	Apple Addresses Issues with iTunes 8.0
September 16	Fake Antivirus Software Circulating
September 16	Apple Releases Security Updates for Multiple Vulnerabilities
September 18	Adobe Releases Security Advisory for Mac Illustrator
September 19	VMware Releases Security Advisory VMSA-0008-0015
September 24	Cisco Releases Security Alerts
September 24	Mozilla Releases Firefox 3.0.2

Current Activity for September 2008	
September 25	Apple Releases Java Updates for Mac OS X 10.4 and 10.5
September 25	Veritas NetBackup Server/Enterprise Server Vulnerabilities
September 26	Multiple Web Browsers Affected by Clickjacking
September 26	Adobe PDF Exploit Toolkits Circulating
September 30	Mozilla Releases Firefox and Thunderbird Updates
September 30	WinZip Releases Version 11.2 SR-1

Technical Cyber Security Alerts

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

Technical Cyber Security Alerts for September 2008	
September 9	TA08-253A Microsoft Updates for Multiple Vulnerabilities
September 16	TA08-260A Apple 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.

Cyber Security Alerts (non-technical) for September 2008	
September 9	SA08-253A Microsoft Updates for Multiple Vulnerabilities
September 16	SA08-260A Apple Updates for Multiple Vulnerabilities

Cyber Security Bulletins

Cyber Security Bulletins are issued weekly and provide a summary of new vulnerabilities that have been 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) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

Security Bulletins for September 2008
SB08-273 Vulnerability Summary for the Week of September 22, 2008
SB08-266 Vulnerability Summary for the Week of September 15, 2008
SB08-259 Vulnerability Summary for the Week of September 8, 2008
SB08-252 Vulnerability Summary for the Week of September 1, 2008
SB08-246 Vulnerability Summary for the Week of August 25, 2008

A total of 449 vulnerabilities were recorded in the NVD during September 2008.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users and are issued every two weeks. September's tips focused on Voice over Internet Protocol (VoIP) and identity theft.

Cyber Security Tips for September 2008	
September 3	ST05-018 Understanding Voice over Internet Protocol
September 16	ST05-019 Preventing and Responding to Identity Theft

Security Highlights

Phishing Scams

US-CERT received reports of multiple phishing scams during the month of September. Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Many of the phishing scams reported this month involved emails that appeared to originate from a legitimate organization or known individual. The emails were designed to entice users into clicking links that would redirect them to fraudulent websites where attackers could then steal financial information.

Phishing attacks often increase following natural disasters or popular news events. For example, US-CERT has received reports of phishing scams and email attacks throughout the United States presidential election campaigns related to the upcoming election. Additionally, US-CERT warned users of potential phishing scams early in the month following Hurricane Gustav.

US-CERT released multiple Current Activity entries to address reports of these scams and to provide mitigation strategies. US-CERT reminds users to remain cautious when receiving unsolicited email messages and to review the following documents available on the US-CERT website:

- Recognizing and Avoiding Email Scams (pdf)
- Avoiding Social Engineering and Phishing Attacks

Clickjacking

US-CERT became aware of public reports of a new cross-browser exploit technique called "Clickjacking." According to one of the reports, with Clickjacking attackers trick users into clicking on something that is barely or momentarily noticeable. Therefore, when users click on a web page, they may actually be clicking on content from another page. A separate report indicated that this flaw affects most web browsers and that no fix was available, although disabling browser scripting and plug-ins may help mitigate some of the risks.

An additional report suggested that Firefox users consider using the NoScript plug-in as an added preventative measure. Disabling IFRAMEs, active content, and plug-ins by default, as outlined in the Securing Your Web Browser document, may protect against the vulnerability. Note, disabling IFRAMES, active content, and plug-ins may reduce the functionality of some websites.

US-CERT released a Current Activity to detail this issue and provide mitigation strategies.

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.

Web Site Address: http://www.us-cert.gov
Email Address: info@us-cert.gov
Phone Number: +1 (888) 282-0870
PGP Key ID: CF5B48C2
PGP Key Fingerprint: 01F1 9C58 0817 D612 45ED 3FCF 3004 FE8C CF5B 48C2
PGP Key: https://www.us-cert.gov/pgp/info.asc