US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary

- February 2008 -

This report summarizes general activity as well as updates made to the National Cyber Alert System for the month of February. 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 February 2008, US-CERT issued 33 current activity updates, three (3) technical cyber security alerts, three (3) cyber security alerts, two (2) cyber security tips, and four (4) weekly cyber security bulletin summary reports.

Highlights for this month include various phishing attacks and multiple software updates issued by Adobe, Apple, Microsoft, Mozilla, and VMware.

Contents

Current Activity

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

- US-CERT received reports of a phishing campaign that used a Department of Justice email template to target as many as 20,000 users across multiple countries.
- Other phishing activity involved fraudulent emails regarding presidential elections, the U.S. Internal Revenue Service, and the lunar eclipse.
- Adobe issued software updates to address multiple vulnerabilities in Adobe Reader and Flash Media Server.
- Apple issued updated versions of Mac OS X, iPhoto, and QuickTime to address vulnerabilities that could allow remote users to execute arbitrary code.
- Microsoft released security updates to address vulnerabilities in MS Windows, Internet Explorer, Office, and Visual Basic. In addition, US-CERT became aware of a fraudulent website that claimed to be a Microsoft Update site, which instead attempted to infect users with malware.
- Mozilla released updated versions of Firefox, Thunderbird, and SeaMonkey to address multiple vulnerabilities including arbitrary code execution, denial of service, cross-site scripting, directory traversal, and information disclosure.
- VMware released a security alert regarding a vulnerability in Windows-hosted VMware Workstation, Player, and ACE that could allow read-write access to the host file system.

Current Activity for February 2008	
February 1	Department of Justice Phishing Campaign
February 4	Publicly Available Exploit for Facebook and MySpace Image Uploader Vulnerability
February 5	Yahoo! Music Jukebox ActiveX Buffer Overflow Vulnerabilities
February 6	Fraudulent Microsoft Update Web Site
February 6	Apple Releases Security Update to Address iPhoto Vulnerability
February 7	Microsoft Releases Advance Notification for February Security Bulletin
February 7	Adobe Reader Update
February 7	Apple QuickTime Update
February 7	Sun Java SE 6 Update
February 8	Microsoft to Release Internet Explorer 7.0 via WSUS
February 11	Mozilla Firefox view-source Information Disclosure Vulnerability
February 11	Trojan Spreading via MSN Messenger
February 11	Mozilla Releases Updates to Address Vulnerabilities in Multiple Products
February 12	Apple Releases Security Updates for Multiple Vulnerabilities
February 12	Active Exploitation of Adobe Reader Vulnerabilities
February 13	Cisco Releases Security Advisories for Vulnerabilities
February 13	Microsoft Releases February Security Bulletin
February 14	Email Attacks Circulating
February 14	Public Exploit for Local Linux Kernel Vulnerability
February 14	Adobe Flash Media Server Vulnerabilities
February 15	Public Exploit Code for Microsoft Works Vulnerabilities
February 18	Mozilla Firefox and Opera Vulnerability
February 21	BEA Releases Security Advisories for Vulnerabilities
February 21	EMC RepliStor Vulnerabilities
February 21	Lunar Eclipse Email Attack
February 21	Symantec Veritas Storage Foundation Update
February 22	Novell iPrint Client Vulnerability
February 25	VMware Releases Security Alert
February 26	Microsoft Windows CE Trojan
February 27	Symantec Releases Security Advisory
February 27	Mozilla Releases Security Advisory
February 28	Opera Releases Update
February 28	Final Netscape Navigator Release

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 February 2008	
February 12	TA08-043A Adobe Reader and Acrobat Vulnerabilities
February 12	TA08-043B Apple Updates for Multiple Vulnerabilities
February 12	TA08-043C 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 computer users can take to protect themselves from attack.

Security Alerts (non-technical)for February 2008	
February 12	SA08-043A Adobe Reader and Acrobat Vulnerabilities
February 12	SA08-043B Apple Updates for Multiple Vulnerabilities
February 12	SA08-043C Microsoft 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 February 2008
SB08-042 Vulnerability Summary for the Week of February 4, 2008
SB08-049 Vulnerability Summary for the Week of February 11, 2008
SB08-056 Vulnerability Summary for the Week of February 18, 2008
SB08-062 Vulnerability Summary for the Week of February 25, 2008

A total of 518 vulnerabilities were recorded in the NVD during February 2008.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users and are issued twice a month. February's tips focused on securing wireless networks and avoiding copyright infringement.

Cyber Security Tips for February 2008	
February 6	ST05-003 Securing Wireless Networks
February 20	ST05-004 Avoiding Copyright Infringement

Security Highlights

Multiple Web Browser Updates

Microsoft Internet Explorer, Mozilla Firefox, Opera, and Netscape Navigator were all updated in February to address various vulnerabilities in these web browsers. Vulnerabilities in various third-party ActiveX controllers impacted Microsoft Internet Explorer. Installing patches for third-party software or disabling the vulnerable ActiveX controllers mitigated these risks. Mozilla issued an update for Firefox version 2.0.12 to fix web forgery overwrite, URL token stealing, privilege escalation, cross-site scripting, remote code execution, and other vulnerabilities. Version 9.2.6 of Opera corrected issues with text input, image properties, and cross-site scripting. In addition, support for Netscape Navigator ended as of March 1, 2008, which effectively retired the browser.

Phishing Trends

U.S. government agency names and logos continue to be used in phishing campaigns to create a false sense of authenticity. In early February, a Department of Justice scam used highly targeted and customized messages posing as complaints filed against individuals. More recently, an Internal Revenue Service scam claimed to offer tax rebates to users in order to obtain their sensitive information. Other phishing attacks claimed to contain links to video clips of newsworthy items, that when opened, would install malware on to the victims' computers.

US-CERT reminds users not to open or respond to unsolicited email. Please refer to Cyber Security Tip ST04-014 – Avoiding Social Engineering (http://www.us-cert.gov/cas/tips/ST04-014.html).

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: 0x7C15DFB9
PGP Key Fingerprint: 673D 044E D62A 630F CDD5 F443 EF31 8090 7C15 DFB9
PGP Key: https://www.us-cert.gov/pgp/info.asc