US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary

- January 2008 -

This report summarizes general activity as well as updates made to the National Cyber Alert System for the month of January. 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 January 2008, US-CERT issued 29 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 a mass phishing campaign using a Department of Justice email template, new Storm Worm variants posing as Valentine's Day and medical spam, and multiple software updates issued by Apple and Microsoft.

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 became aware of a phishing campaign using a Department of Justice email template, which targeted 20,000 individuals across multiple sectors and countries.
- New variations of Storm Worm activity using romantic or Valentine's Day greetings with links to malicious websites were detected. Another variant contained a link to a website containing spam about medical information.
- Adobe issued security bulletins to address multiple cross-site scripting vulnerabilities in Adobe Dreamweaver, Adobe Contribute, and Adobe Connect Enterprise Server.
- A broken cable in the Mediterranean Sea interrupted internet and voice communications to several countries in the Middle East and South Asia.
- Microsoft released security updates to address vulnerabilities in TCP/IP communication and the Local Security Authority Subsystem Service (LSASS) across a variety of Windows software.
- Apple released updated versions of QuickTime, iPhone, and iPod touch to address multiple vulnerabilities in these products.

Current Activity for January 2008	
January 2	Publicly Available Exploit Code for RealPlayer
January 3	Flash File Cross-Site Scripting Vulnerabilities
January 3	Microsoft Releases Advance Notification for January Security Bulletin
January 8	Microsoft Releases January Security Bulletin
January 9	New iPhone Trojan Spreading
January 10	Widespread SQL Injection Attacks Compromising Websites
January 11	QuickTime Real Time Streaming Protocol Vulnerability
January 15	Attack Vector Targets UPnP
January 15	Fraudulent Mac OS Security Tool Circulating
January 16	New Storm Worm Variant Spreads
January 16	Microsoft Office Excel Remote Code Vulnerability
January 16	Apple Releases Security Updates to Address Multiple Vulnerabilities
January 17	Cisco Releases Security Advisory to Address Vulnerability in Cisco Unified Communication Manager
January 17	Oracle Releases Critical Patch Update for January 2008
January 17	Adobe Releases Security Bulletins to Address Multiple Cross-Site Scripting Vulnerabilities
January 18	Citrix Releases Update to Address Vulnerability
January 18	Skype Releases Security Bulletin to Address Cross Zone Scripting Vulnerability
January 22	SymbianOS Worm
January 23	Cisco Releases Security Advisories to Address Vulnerabilities in PIX, ASA, and AVS
January 24	Microsoft Security Bulletin Re-Releases and Revisions
January 24	Mozilla Firefox Chrome Vulnerability
January 24	Sun Releases Java Update
January 25	IBM AIX Vulnerabilities
January 25	GE Fanuc Product Vulnerabilities
January 30	Cisco Releases Security Advisories to Address a Vulnerability in the Cisco Wireless Control System
January 31	Storm Worm Directing Users to Medical Spam Web Sites
January 31	Communication Interruption Due to Mediterranean Cable Break
January 31	Possible Department of Justice Phishing Campaign

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 January 2008	
January 8	TA08-008A Microsoft Updates for Multiple Vulnerabilities
January 16	TA08-016A Apple QuickTime Updates for Multiple Vulnerabilities
January 17	TA08-017A Oracle 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 January 2008	
January 8	SA08-008A Microsoft Updates for Multiple Vulnerabilities
January 16	SA08-016A Apple QuickTime 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 January 2008
SB08-014 Vulnerability Summary for the Week of January 7, 2008
SB08-021 Vulnerability Summary for the Week of January 14, 2008
SB08-028 Vulnerability Summary for the Week of January 21, 2008
SB08-035 Vulnerability Summary for the Week of January 28, 2008

A total of 498 vulnerabilities were recorded in the NVD during January 2008.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users and are issued twice a month. January’s tips focused on evaluating a web browser’s security settings and keeping children safe online. Links to the full versions of these documents are listed below.

Cyber Security Tips for January 2008	
January 10	ST05-001 Evaluating Your Web Browser's Security Settings
January 23	ST05-002 Keeping Children Safe Online

Security Highlights

US-CERT reported on two incidents of malware targeting well-known mobile phones. These two incidents highlight the need to protect your mobile devices and remain vigilant against unknown messages, prompts, or files.

The first incident involved a Trojan targeting Apple iPhone users. Viewed as more of a prank than an actual threat, the Trojan reportedly targeted iPhones that had been modified to allow for the installation of third-party applications. The website hosting the malware was quickly removed, but the incident still highlighted the importance of securing mobile devices.

In a separate incident, a worm surfaced that was targeting mobile devices running SymbianOS. The worm, dubbed SymbOS/Beselo.A!, disguises itself under media file extensions with names such as Beauty.jpg, Sex.mp3 and Love.rm.

For more information, refer to the full current activity entry. Additional information on protecting your mobile devices can be found in US-CERT Cyber Security Tip ST04-020, "Protecting Portable Devices: Data Security."

In late January, US-CERT reported on a spear phishing campaign that involved targeted email messages claiming to be from the Department of Justice (DOJ). The messages were designed to convince recipients that they were the subject of a business complaint filed through the DOJ. The Department of Justice released a statement on their website indicating that they do not, and would not send this type of information via email.

US-CERT reminds users not to open attachments or links included in unsolicited email messages. More information on how to avoid becoming a victim of such an attack can be found in the US-CERT Cyber Security Tips Using Caution with Email Attachments and Avoiding Social Engineering and Phishing Attacks.

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