US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary

- January 2009 -

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 2009, US-CERT issued 16 Current Activity entries, four (4) Technical Cyber Security Alerts, two (2) Cyber Security Alerts, four (4) weekly Cyber Security Bulletins, and two (2) Cyber Security Tips.

Highlights for this month included advisories released by Cisco, BlackBerry, Symantec, Microsoft, Apple, and Oracle; the Win32/ Conficker/ Downadup Worm; and phishing scams centered around the Israeli/Hamas conflict, the Presidential Inauguration, and the upcoming Valentine's Day.

Contents

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.

- Cisco released Security Advisories, cisco-sa-20090107-gss and cisco-sa-20090114-ironport, to address vulnerabilities in Global Site Selector and Iron Port products respectively. These vulnerabilities may allow a remote attacker to cause a denial-of-service condition and allow an unauthorized attacker to view the contents of secure email or gain access to the administration interface.
- Research In Motion released Security Advisories KB17118 and KB17119 to address vulnerabilities in the PDF Distiller of the BlackBerry Attachment Service for BlackBerry Unite and BlackBerry Enterprise Server. The vulnerabilities are due to the improper processing of PDF files within the Distiller component of the BlackBerry Attachment Service. By convincing a user to open a maliciously crafted PDF attachment on a BlackBerry smartphone, an attacker may be able to execute arbitrary code on the system running the BlackBerry Attachment Service.

- Symantec released a security advisory to address a vulnerability in the Symantec AppStream LaunchObj ActiveX control. By convincing a user to view a specially crafted HTML document, an attacker may be able to execute arbitrary code with the privileges of the user. Additional details can be found in US-CERT Vulnerability Note VU#194505.
- Microsoft released its January Security Bulletin Summary. This bulletin included an update to address vulnerabilities in the Server Message Block (SMB) Protocol that affects all supported versions of Microsoft Windows. A remote, unauthenticated attacker could gain elevated privileges, execute arbitrary code, or cause a denial of service.
- Apple has released QuickTime 7.6 to address multiple vulnerabilities in Windows and Mac OS X systems. These vulnerabilities may allow a remote attacker to execute arbitrary code or cause a denial-of-service condition. US-CERT encourages users to review Apple Article HT3403 and upgrade to QuickTime 7.6.
- Oracle released a Critical Patch Update for January, which addressed 41 vulnerabilities in nine software products. These products include Oracle Database, Secure Backup, Application Server, PeopleSoft, JDEdwards Suite, BEA Product Suite, and others. Potential impacts of these vulnerabilities include the execution of arbitrary code or commands, information disclosure, and denial of service. Additional details can be found in US-CERT Technical Cyber Security Alert TA09-015A.

Current Activity for January 2009	
January 8	OpenSSL Releases Security Advisory
January 8	Cisco Releases Security Advisory for Global Site Selector
January 8	Microsoft Releases Advance Notification for January Security Bulletin
January 9	Malicious Code Circulating via Israel/Hamas Conflict Spam Messages
January 12	Oracle Issues Pre-Release Announcement for January Critical Patch Update
January 13	BlackBerry Security Advisories
January 13	Microsoft Releases January Security Bulletin
January 13	Oracle Releases Critical Patch Update for January 2009
January 15	Cisco Releases Security Advisory for IronPort Encryption Appliance and IronPort PXE Encryption product
January 15	Spam, Phishing, and Malware Related to Presidential Inauguration
January 16	Symantec Releases Security Advisory
January 16	Widespread Infection of Win32/Conficker/Downadup Worm
January 21	Cisco Releases Security Advisory for Cisco Security Manager
January 21	Apple Releases QuickTime 7.6
January 29	Malicious Code Spreading Via Valentine's Day Spam
January 30	Novell Releases Updates for GroupWise

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 2009	
January 13	TA09-013A Microsoft Updates for Multiple SMB Protocol Vulnerabilities
January 15	TA09-015A Oracle Updates for Multiple Vulnerabilities
January 20	TA09-020A Microsoft Windows Does Not Disable AutoRun Properly
January 22	TA09-022A Apple QuickTime 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 January 2009	
January 13	SA09-013A Microsoft Updates for Multiple Vulnerabilities
January 22	SA09-022A 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 2009
SB09-005 Vulnerability Summary for the Week of December 29, 2008
SB09-012 Vulnerability Summary for the Week of January 5, 2009
SB09-019 Vulnerability Summary for the Week of January 12, 2009
SB09-026 Vulnerability Summary for the Week of January 19, 2009

A total of 467 vulnerabilities were recorded in the NVD during January 2009.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users and are issued every two weeks. January's tips focused on corrupted software files, and protecting cell phones and personal digital assistants (PDAs) from attacks.

Cyber Security Tips for January 2009	
January 7	ST06-006 Understanding Hidden Threats: Corrupted Software Files
January 28	ST06-007 Defending Cell Phones and PDAs Against Attack

Security Highlights

Widespread Infection of Win32/Conficker/Downadup Worm
Public reports indicated a widespread infection of the Win32/Conficker/Downadup worm, possibly affecting several million systems. This worm exploits a previously patched vulnerability in the Microsoft Windows Server service, which was addressed in Microsoft Security Bulletin MS08-067. This vulnerability involves a stack buffer overflow condition when handling Remote Procedure Call (RPC) messages. A remote, unauthenticated attacker may be able to execute arbitrary code with SYSTEM privileges on a vulnerable system by sending a specially crafted RPC request. Multiple versions of the Windows operating system are affected, including Windows 2000, Server 2003, XP, Vista, and Server 2008.

This worm can propagate through multiple methods, including removable media. The worm thrives in environments that have open Windows shares, weak passwords, a lack of current software updates and unrestricted AutoRun functionality for removable media. US-CERT strongly encourages users to disable AutoRun as described in US-CERT Technical Cyber Security Alert TA09-020A and review Microsoft Security Bulletin MS08-067. Unpatched systems should be updated as soon as possible.

Spam and Phishing Trends
Early in January, US-CERT became aware of public reports of malicious code circulating via spam email messages related to the Israel/Hamas conflict in Gaza. These messages may have contained factual information about the conflict and appeared to have originated from CNN. Additionally, the messages indicated that further news coverage of the conflict could be viewed via a link provided in the body of the email. Users who clicked on this link were redirected to a bogus CNN website that appeared to contain the video. Users who attempted to view this video would have been prompted to update to a new version of Adobe Flash Player to view it. The fraudulent update was actually malicious code that may have been installed on their systems.

Later in the month, US-CERT received reports of an increased number of phishing sites and spam related to the upcoming Presidential Inauguration. This was consistent with previous phishing and spamming campaigns that often coincide with highly publicized events. Similar to other phishing scams, a link to a video about the topic was included in the message to lure users into installing malicious code disguised as a Flash Player update.

With the approach of Valentine's Day, US-CERT became aware of public reports of malicious code circulating via spam email messages with a Valentine theme. These messages included a link to a website that contained several images of hearts and instructed users to select one image. If users clicked on an image, they would have been prompted to download an executable file. Reports indicated that the executable files could be named: youandme.exe, onlyyou.exe, you.exe, and meandyou.exe (although file names may change at any time). If users accepted the download, malicious code may have been installed on their systems.

US-CERT encourages users to take the following preventative measures to help mitigate the security risks associated with phishing scams:

- Install antivirus software, and keep virus signatures up to date.
- Do not follow unsolicited links and do not open unsolicited email messages.
- Use caution when visiting untrusted websites.

- Use caution when downloading and installing applications.
- 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.

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