US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary
- February 2009 -

This report summarizes general activity as well as updates made to the National Cyber Alert System for February 2009. 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 February 2009, US-CERT issued 16 Current Activity entries, two (2) Technical Cyber Security Alerts, two (2) Cyber Security Alerts, four (4) weekly Cyber Security Bulletins, and one (1) Cyber Security Tip.

Highlights for this month included advisories released by Cisco, Microsoft, Apple, Mozilla, Hewlett-Packard, RIM, and Adobe, active exploitation of Internet Explorer 7, and propagation of a new variant of the Conficker/Downadup worm.

Contents

Current Activity

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

- Cisco released multiple security advisories. Security advisory cisco-sa-20090204-wlc addressed multiple vulnerabilities in Cisco Wireless LAN Controllers that could allow an attacker to cause a denial-of-service condition or operate with escalated privileges. Security Advisory cisco-sa-20090225-ace addressed multiple vulnerabilities in the ACE Application Control Engine Module, ACE 4710 Application Control Engine. These vulnerabilities may allow an attacker to obtain administrative level access, operate with escalated privileges, or cause a denial-of-service condition.
- Microsoft released its February Security Bulletin to address vulnerabilities in Microsoft Windows, Office, Internet Explorer, Exchange Server, and SQL Server. These vulnerabilities may allow an attacker to execute arbitrary code.
    - Additionally, Microsoft released Security Advisory 968272 to address reports of a vulnerability in Microsoft Office Excel. By convincing a user to open a specially crafted Excel document, an attacker may be able to execute arbitrary code.

  - A public report indicated active exploitation of a previously patched vulnerability in Microsoft Internet Explorer 7. This vulnerability was addressed in Microsoft Security Advisory MS09-002. Additional information is available in US-CERT Technical Cyber Security Alert TA09-041A.

- Apple released Security Update 2009-001, Java for Mac OS X 10.5 Update 3, Java for Mac OS X 10.4 Release 8, and Safari 3.2.2 for Windows. These security updates addressed vulnerabilities that could allow an attacker to execute arbitrary code, cause a denial-of-service condition, access the system with escalated privileges, or obtain sensitive information.

- Mozilla has released Firefox 3.0.6 to address multiple vulnerabilities. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code, obtain sensitive information, or conduct cross-site scripting attacks. As described in the Mozilla Foundation Security Advisories, some of these vulnerabilities may also affect Thunderbird and SeaMonkey.

- Research In Motion (RIM) released Security Advisory KB16248 to address a vulnerability in the BlackBerry Application Web Loader 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. The attacker could also cause Internet Explorer to crash.

Current Activity for February 2009	
February 2	VMware Releases Security Advisory
February 4	Cisco Releases Security Advisory for Cisco Wireless LAN Controllers
February 4	Mozilla Releases Firefox Updates
February 5	Microsoft Releases Advanced Notification for February Security Bulletin
February 6	IRS Stimulus Package Phishing Scam
February 6	HP Releases Security Bulletin for HP OpenView Network Node Manager
February 9	HP Releases Security Bulletin to Address a Vulnerability in Multiple Printers
February 10	BlackBerry Security Advisory
February 10	Microsoft Releases February Security Bulletin Summary
February 17	Active Exploitation of Microsoft Internet Explorer 7 Vulnerability
February 17	Apple Releases Security Updates
February 20	Adobe Releases Security Bulletin for Critical Vulnerability
February 23	New Variant of Conficker/Downadup Worm Circulating
February 24	Microsoft Releases Security Advisory (968272)
February 25	Adobe Releases Security Bulletin for Flash Player
February 27	Cisco Releases Security Advisory for ACE 4710 Appliance and ACE Module

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 2009	
February 10	TA09-041A Microsoft Updates for Multiple Vulnerabilities
February 20	TA09-051A Adobe Acrobat and Reader Vulnerability

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 February 2009	
February 10	SA09-041A Microsoft Updates for Multiple Vulnerabilities
February 20	SA09-051A Adobe Acrobat and Reader Vulnerability

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 2009
SB09-033 Vulnerability Summary for the Week of January 26, 2009
SB09-040 Vulnerability Summary for the Week of February 2, 2009
SB09-047 Vulnerability Summary for the Week of February 9, 2009
SB09-054 Vulnerability Summary for the Week of February 16, 2009

A total of 688 vulnerabilities were recorded in the NVD during February 2009.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users and are issued every two weeks. February's tips focused on safeguarding sensitive personal and work data.

Cyber Security Tips for February 2009	
February 18	ST06-008 - Safeguarding Your Data

Security Highlights

Multiple Adobe Updates

Adobe released security bulletins to alert users of vulnerabilities in multiple products. Adobe Security Bulletin APSA09-01 addressed a vulnerability that may allow an attacker to execute arbitrary code or cause a denial-of-service condition in Reader and Acrobat. Adobe indicated reports of active exploitation. The buffer overflow vulnerability occurs when Adobe Reader and Acrobat handle files with specially crafted JBIG2 streams. Acrobat integrates with popular web browsers, and visiting a website is usually sufficient to cause Acrobat to load PDF content. An attacker could exploit these vulnerabilities by convincing a user to load a specially crafted Adobe Portable Document Format (PDF) file. US-CERT also released VU#905281 and TA09-051A to provide further details.

- Disable JavaScript in Adobe Reader and Acrobat. Acrobat JavaScript can be disabled in the General preferences dialog (Edit, Preferences, JavaScript, and un-check "Enable Acrobat JavaScript").
- Prevent Internet Explorer from automatically opening PDF documents.
- Disable the ability to display PDF documents in the web browser. This can be disabled in the General preferences dialog (Edit, Preferences, Internet, and un-check "Display PDF in browser").
- Use caution when opening untrusted PDF files.
- Install antivirus software, and keep virus signatures up to date.

Adobe also released Security Bulletin APSB09-01 to address multiple vulnerabilities in Flash Player that could allow an attacker to execute arbitrary code, cause a denial of service condition, conduct Clickjacking attacks, or operate with escalated privileges. US-CERT encourages users to review Adobe Security Bulletin APSB09-01 and upgrade to Flash Player 10.0.22.87 to help mitigate the risks.

New Variant of Conficker/Downadup Worm Circulating

Public reports circulated concerning a new variant of the Conficker/Downadup worm, named Conficker B++. This variant propagates itself via multiple methods, including exploitation of the previously patched vulnerability addressed in MS08-067, password guessing, and the infection of removable media. Most significantly, Conficker B++ implemented a new backdoor with "auto-update" functionality, which allows machines compromised by the new variant to have additional malicious code installed on them. According to Microsoft, there is no indication that systems infected with previous variants of Conficker can automatically be re-infected with the B++ variant.

US-CERT strongly encourages users to review Microsoft Security Bulletin MS08-067 and update unpatched systems as soon as possible.

Additionally, US-CERT recommends that users take the following preventative measures to help mitigate the security risks:

- Install antivirus software, and keep the virus signatures up to date.
- Review the Microsoft Malware Protection Center blog entry for details regarding the worm.
- Review the Using Caution with USB Drives Cyber Security Tip for more information on protecting removable media.

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