US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary
- March 2009 -

This report summarizes general activity as well as updates made to the National Cyber Alert System for March 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 March 2009, US-CERT issued 17 Current Activity entries, two (2) Technical Cyber Security Alerts, two (2) Cyber Security Alerts, five (5) weekly Cyber Security Bulletins, and one (1) Cyber Security Tip.

Highlights for this month included updates released by Microsoft, Mozilla, Adobe, Cisco, and Sun to address multiple vulnerabilities; and potential propagation of Waledac and Conficker malware.

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.

- The Microsoft Security Bulletin for March addressed multiple vulnerabilities in the Windows Operating System. A vulnerability in the Windows kernel could allow remote code execution, while vulnerabilities in SChannel, DNS, and WINS Server could allow spoofing.
- Mozilla Foundation has released Firefox 3.0.7 to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, obtain sensitive information, or spoof the location bar. These vulnerabilities also affect Thunderbird and SeaMonkey. Subsequently, Mozilla Foundation has released Firefox 3.0.8 to address two more vulnerabilities that also affected SeaMonkey.
- Adobe released Reader 9.1 and Acrobat 9.1 to address a buffer overflow condition that exists in the way Adobe Acrobat Reader handles JBIG2 streams. Exploitation of this vulnerability may allow a remote attacker to execute arbitrary code or cause a denial-of-service condition. Adobe acknowledged reports of active exploitation of this vulnerability. Additional information is

described in Adobe security bulletin APSB09-03 and in the US-CERT Vulnerability Notes Database.

- Cisco released multiple security advisories to address vulnerabilities in its IOS Software. These vulnerabilities may allow an attacker to cause a denial-of-service condition, interfere with network traffic, or operate with escalated privileges. Additional details are included in the following advisories: cisco-sa-20090325-udp; cisco-sa-20090325-tcp; cisco-sa-20090325-ip; cisco-sa-20090325-webvpn; cisco-sa-20090325-mobileip; cisco-sa-20090325-scp; cisco-sa-20090325-sip; cisco-sa-20090325-ctcp

- Sun Microsystems released an alert to address multiple vulnerabilities in the Java System Identity Manager. These vulnerabilities may allow an attacker to execute arbitrary commands, conduct cross-site scripting attacks, modify configuration settings, or obtain sensitive information. US-CERT encourages users and administrators to review Sun Alert 253567 and apply any necessary patches.

Current Activity for March 2009	
March 3	Opera Software Releases Opera Browser 9.64
March 4	Malicious Code Targeting Social Networking Site Users
March 5	Mozilla Foundation Releases Firefox 3.0.7
March 5	Microsoft Releases Advanced Notification for March Security Bulletin
March 5	Economic Stimulus Email and Website Scams
March 10	Microsoft Releases March Security Bulletin Summary
March 10	New Attack Vectors for Adobe JBIG2 Vulnerability
March 11	Adobe Releases Security Updates for Reader 9 and Acrobat 9
March 17	Waledac Trojan Horse Spam Campaign Circulating
March 18	Autonomy KeyView SDK Vulnerability
March 18	Adobe Releases Security Bulletin
March 23	Sun Releases Alert for Java System Identity Manager Vulnerabilities
March 25	Cisco Releases Multiple Security Advisories for IOS Vulnerabilities
March 26	OpenSSL Releases Security Advisory
March 26	Sun Releases Updates for Java SE
March 30	Mozilla Foundation Releases Firefox 3.0.8
March 30	Conficker Worm Targets Microsoft Windows Systems

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 March 2009	
March 10	TA09-069A Microsoft Updates for Multiple Vulnerabilities
March 29	TA09-088A Conficker Worm Targets Microsoft Windows Systems

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 March 2009	
March 10	SA09-069A Microsoft Updates for Multiple Vulnerabilities
March 29	SA09-088A Conficker Worm Targets Microsoft Windows Systems

Cyber Security Bulletins

Cyber Security Bulletins are issued weekly and provide a summary of new vulnerabilities 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 March 2009
SB09-061 Vulnerability Summary for the Week of February 23, 2009
SB09-068 Vulnerability Summary for the Week of March 2, 2009
SB09-075 Vulnerability Summary for the Week of March 9, 2009
SB09-083 Vulnerability Summary for the Week of March 16, 2009
SB09-090 Vulnerability Summary for the Week of March 23, 2009

A total of 554 vulnerabilities were recorded in the NVD during March 2009.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users and are issued every two weeks. March's tip focused on coordinating virus and spyware defense.

Cyber Security Tips for March 2009	
March 18	ST06-009 Coordinating Virus and Spyware Defense

Security Highlights

Waledac Trojan

US-CERT received public reports of malicious code circulating via spam email messages related to bogus terror attacks in the recipient's local area. These messages used subject lines implying that a fatal bomb attack had occurred near the recipient and contained a link to “breaking news.” Users who clicked on the link would instead be taken to a site posing as a Reuters news article that contained a false story regarding the attack. The systems serving the fake story checked a visiting user’s IP address to obtain a geographical location to insert a nearby place’s name into the article. The articles also contained links to video content, claiming that the latest Flash Player was required to view the video. If users attempted to update or install the Flash Player from the link provided in the article, their systems could have been infected with malicious code. US-CERT released a Current Activity entry describing this spamming campaign.

New Variant of Conficker/Downadup Worm Circulating

Public reports indicated a widespread infection of the Conficker/Downadup worm, which can infect a Microsoft Windows system from a thumb drive, a network share, or directly across a corporate network, if the network servers are not patched with the MS08-067 patch from Microsoft. US-CERT released an updated Current Activity entry when researchers discovered a new variant of the Conficker Worm. This variant updates earlier infections via its peer-to-peer (P2P) network as well as resuming scan-and-infect activity against unpatched systems. This variant appears to download additional malicious code onto victim systems, possibly including copies of the Waledac Trojan, a spam-oriented malicious application that previously propagated exclusively via false email messages that contained malicious links.

Home users can apply a simple test for the presence of a Conficker/Downadup infection on their home computers. The presence of a Conficker/Downadup infection may be detected if a user is unable to surf to certain security solution websites:

http://www.symantec.com/norton/theme.jsp?themeid=conficker_worm&inid=us_ghp_link_conficker_worm
http://www.microsoft.com/protect/computer/viruses/worms/conficker.mspx
http://www.mcafee.com

If a user is unable to reach any of these websites, it may indicate a Conficker/Downadup infection. The infection interferes with queries for these sites, preventing a user from connecting to them. If a Conficker/Downadup infection is suspected, the system or computer should be removed from the network or, for home users, unplugged from the internet.

Instructions, support and more information on how to manually remove a Conficker/Downadup infection from a system have been published by major security vendors. Please see below for a few of those sites, and for the number of the Microsoft PC Safety hotline. Each of these vendors offers free tools that can verify the presence of a Conficker/Downadup infection and remove the worm:

http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-011316-0247-99
http://support.microsoft.com/kb/962007
http://www.microsoft.com/protect/computer/viruses/worms/conficker.mspx
Microsoft PC Safety hotline at 1-866-PCSAFETY

Conficker/Downadup infections can be prevented by implementing the MS08-067 patch (see http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx), disabling the AutoRun functionality (see http://www.us-cert.gov/cas/techalerts/TA09-020A.html), and maintaining up-to-date antivirus software.

US-CERT encourages users to take the following preventative measures to help prevent a Conficker/Downadup infection:

- Ensure all systems have the MS08-067 patch.
- Disable AutoRun functionality. See US-CERT Technical Cyber Security Alert TA09-020A.
- Maintain up-to-date antivirus software.
- 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.
- Obtain software applications and updates directly from the vendor's website.
- 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