US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary
- November 2008 -

This report summarizes general activity as well as updates made to the National Cyber Alert System for the month of November. 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 November 2008, US-CERT issued 18 Current Activity entries, three (3) Technical Cyber Security Alerts, three (3) Cyber Security Alerts, four (4) weekly Cyber Security Bulletins, and two (2) Cyber Security Tips.

Highlights for this month included updates released by Adobe, Apple, Microsoft, Mozilla, and VMware; increased activity regarding the Torpig Trojan horse; malicious code spreading via USB drives; and phishing attacks related to the presidential election and the Federal Reserve.

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.

- Adobe released Security Bulletins APS08-19, APSB08-20, and APSB08-23 to address vulnerabilities in Adobe Reader and Acrobat, Flash Player, and AIR, respectively. Additionally, US-CERT became aware of public reports of active exploitation of the Adobe Reader JavaScript buffer overflow vulnerability reported in Security Bulletin APS08-19.
- Apple released multiple updates for iLife, Safari, iPhone and iPod touch. Safari 3.2 addressed multiple vulnerabilities that could allow an attacker to execute arbitrary code, cause a denial-of-service condition, or obtain sensitive information as described in Apple Article HT3298. Apple iLife Support 8.3.1 addressed multiple vulnerabilities that may allow an attacker to execute arbitrary code or cause a denial-of-service condition (HT3276). Apple also released OS 2.2 for the iPhone and iPod touch to address multiple vulnerabilities that affect CoreGraphics, ImageIO, Networking, Office Viewer, Password Lock, Safari, and Webkit. Exploitation of these vulnerabilities could allow an attacker to execute arbitrary code, place arbitrary calls, cause a denial-of-service condition, spoof user interface, and obtain sensitive information (HT3318).

- US-CERT became aware of public reports of a worm circulating that has the capability of exploiting the recently patched vulnerability described in Microsoft Security Bulletin MS08-067. Microsoft's November Security Bulletin addressed vulnerabilities in MS Windows XML Core Services and MS Server Message Block Protocol that could allow an attacker to perform remote code execution.
- Mozilla released Firefox 2.0.0.18, Firefox 3.0.4, and SeaMonkey 1.1.13 to address multiple vulnerabilities; including arbitrary code execution, privilege escalation, security bypass, cross-site scripting, denial of service, and information disclosure. Some of these vulnerabilities may also affect Thunderbird. Details were published in the Mozilla Foundation security advisories.
- US-CERT became aware of public reports of a high volume of financial accounts compromised by the Torpig (aka Sinowal or Anserin) Trojan horse. This Trojan horse uses HTML injection to add fields to web pages to convince users to provide additional user credentials or financial account information. Compromised systems were being used by attackers to obtain FTP credentials, email addresses, and digital certificates of the current user.

Current Activity for November 2008	
November 3	Sprint Nextel - Cogent Communications Depeering Issue
November 3	Worm Exploiting Microsoft MS08-067 Circulating
November 4	Adobe Releases Security Bulletin
November 6	Torpig Trojan Horse Attack Activity
November 6	Adobe Releases Security Bulletin to Address Flash Player Vulnerabilities
November 6	United States Presidential Election Email Attack
November 7	Microsoft Releases Advance Notification for November Security Bulletin
November 7	Adobe Reader Exploit Circulating
November 10	VMware Releases Security Advisory VMSA-2008-0018 and Updates VMSA-2008-0016.1
November 11	Microsoft Releases November Security Bulletin
November 12	Apple Releases iLife Support 8.3.1
November 13	U.S. Federal Reserve Fraudulent Email Scam
November 13	Mozilla Releases Updates to Address Vulnerabilities in Multiple Products
November 14	Apple Releases Security Updates for Safari
November 18	Adobe Releases Update for AIR
November 20	Malicious Code Spreading Through USB Flash Drive Devices
November 21	Symantec Releases Security Advisory for Backup Exec
November 24	Apple Releases iPhone OS 2.2 and iPhone OS for iPod touch 2.2

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 November 2008	
November 4	TA08-309A Adobe Reader and Acrobat Vulnerabilities
November 11	TA08-316A Microsoft Updates for Multiple Vulnerabilities
November 14	TA08-319A Mozilla 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 November 2008	
November 4	SA08-309A Adobe Reader and Acrobat Vulnerabilities
November 11	SA08-316A Microsoft Updates for Multiple Vulnerabilities
November 14	SA08-319A Mozilla 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 November 2008
SB08-308 Vulnerability Summary for the Week of October 27, 2008
SB08-315 Vulnerability Summary for the Week of November 3, 2008
SB08-322 Vulnerability Summary for the Week of November 10, 2008
SB08-329 Vulnerability Summary for the Week of November 17, 2008

A total of 437 vulnerabilities were recorded in the NVD during November 2008.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users and are issued every two weeks. November's tips focused on USB drives and cyberbullies.

Cyber Security Tips for November 2008	
November 4	ST08-001 Using Caution with USB Drives
November 20	ST06-005 Dealing with Cyberbullies

Security Highlights

Malware Propagating via USB Drives

Due to the portability, availability, and low cost of USB drives, they are popular for storing and transporting files from one computer to another. However, these same characteristics also make them appealing to attackers. In November, US-CERT became aware of public reports of an increase in malicious code propagating via USB flash drive devices. Two popular methods of infecting USB flash drives with malicious code were identified, although these are not the only two methods available.

The first of these methods is referred to as simple file copy. This means that the malicious code initially resides on an infected computer and copies itself to all the storage devices connected to the affected computer. This method requires the user to access the USB flash drive and execute the malicious code.

The second method is referred to as AutoRun.inf modification. In this case, the malicious code alters or creates an autorun.inf file on targeted storage devices connected to the affected computer. When an infected USB flash drive is connected to another computer, the malicious code can be automatically executed with no additional user interaction.

US-CERT issued a Current Activity entry to address this issue and encourages users to review Cyber Security Tip ST08-001, Using Caution with USB Drives, and CERT's Vulnerability Analysis Blog entry, The Dangers of Windows AutoRun, for recommendations to help mitigate the risks.

Phishing Scams Targeting Presidential Elections and the Federal Reserve

US-CERT issued a Current Activity entry early in the month after becoming aware of public reports of email attacks circulating related to the US presidential election. The email messages appeared to be from a seemingly legitimate source with a link to a website that appeared to contain a video of the president elect. The website instructed users to update to a new version of Adobe Flash Player to view the video. This fraudulent update was actually an executable file that could install malicious code on users' systems.

A week later, US-CERT issued a Current Activity entry about a phishing scam involving emails that appeared to originate from the US Federal Reserve. The email messages described a phishing scam and provided links for users to follow to obtain additional information about the alleged scam. Users who followed the links were redirected to a malicious website where a PDF exploit could be used to install malicious code on their systems.

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.

Website 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