US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary

- December 2007 -

This report summarizes general activity as well as updates made to the National Cyber Alert System for the month of December. 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 December 2007, US-CERT issued thirteen (13) current activity updates, three (3) technical cyber security alerts, three (3) cyber security alerts (non-technical), two (2) cyber security tips, and four (4) weekly cyber security bulletin summary reports.

Highlights for the month include new Storm Worm activity, multiple vulnerabilities in Adobe Flash, Apple Mac OS X, and Microsoft Windows.

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.

- Storm Worm variants with holiday-themed subject lines and filenames have become prevalent this season. Additional details are provided in the link below and Security Highlights section.

Current Activity for December 2007	
December 4	Microsoft Releases Security Advisory to Address Web Proxy Auto-Discovery Vulnerability
December 5	Cisco Releases Security Documents for Vulnerabilities
December 6	Microsoft Releases Advance Notification for December Security Bulletin
December 10	Active Exploitation Using Malicious Microsoft Access Databases
December 12	Microsoft Releases December Security Bulletins
December 14	HP Info Center Software Public Exploit Code
December 14	Apple Releases Security Update to Address Multiple Vulnerabilities in QuickTime

Current Activity for December 2007	
December 19	MSRC Releases Update to MS07-069
December 19	Cisco Releases Security Advisory to Address Vulnerability
December 19	Apple Releases Security Updates to Address Multiple Vulnerabilities
December 20	Google Orkut Worm
December 21	Adobe Flash Player Vulnerabilities
December 27	Storm Worm Activity Increases During Holiday Season

Technical Cyber Security Alerts

Technical Cyber Security Alerts are distributed to provide timely information about current security issues, vulnerabilities, and exploits.

- Microsoft released security updates to address vulnerabilities in Windows, DirectX, DirectShow, Windows Media Format Runtime, Internet Explorer, and Web Proxy Auto-Discovery (WPAD).

- Apple released security updates for Mac OS X vulnerabilities involving Adobe Flash, Adobe Shockwave, and GNU Tar third party applications. Apple also released security updates for its Apple QuickTime multimedia application for Mac OS X and Microsoft Windows.

- Multiple vulnerabilities in Adobe's Flash Player were noted that could allow remote attackers to control computers that execute maliciously crafted SWF files. Additional issues regarding these vulnerabilities are being identified in January.

Technical Cyber Security Alerts for December 2007	
December 11	TA07-345A Microsoft Updates for Multiple Vulnerabilities
December 18	TA07-352A Apple Updates for Multiple Vulnerabilities
December 21	TA07-355A Adobe 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 for December 2007	
December 11	SA07-345A Microsoft Updates for Multiple Vulnerabilities
December 18	SA07-352A Apple Updates for Multiple Vulnerabilities
December 21	SA07-355A Adobe 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 December 2007
Vulnerability Summary for the Week of December 3, 2007
Vulnerability Summary for the Week of December 10, 2007
Vulnerability Summary for the Week of December 17, 2007
Vulnerability Summary for the Week of December 24, 2007

A total of 434 vulnerabilities were recorded in the NVD during December 2007.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users and are issued twice a month. December's tips focused on shopping safely online and understanding Internet Service Providers (ISPs). Links to the full versions of these documents are listed below.

Cyber Security Tips for December 2007	
December 12	ST07-001 - Shopping Safely Online
December 27	ST04-024 - Understanding ISPs

Security Highlights

New Variants of StormWorm Appeared Over the Holiday Season

On December 27, US-CERT noted an increase in Storm Worm related activity. The latest activity was centered on messages related to the New Year. This Trojan is spread via unsolicited email messages that contain links to malicious web sites. When the malicious links are followed, the Trojan attempts to exploit unpatched vulnerabilities to install malicious code on a user's system.

US-CERT urges users and administrators to take the following preventative measures to mitigate the security risks:

- Install anti-virus software, and keep its virus signature files up-to-date.
- Block executable and unknown file types at the email gateway.
- Refer to the Recognizing and Avoiding Email Scams 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: 0x7C15DFB9
PGP Key Fingerprint: 673D 044E D62A 630F CDD5 F443 EF31 8090 7C15 DFB9
PGP Key: https://www.us-cert.gov/pgp/info.asc