US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary

- May 2008 -

This report summarizes general activity as well as updates made to the National Cyber Alert System for the month of May. 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 May 2008, US-CERT issued 17 current activity entries, four (4) technical cyber security alerts, three (3) cyber security alerts, four (4) weekly cyber security bulletin summary reports, and two (2) cyber security tips.

Highlights for this month include advisories and updates to address vulnerabilities in Common Data Format (CDF), Debian and Ubuntu Linux operating systems, Adobe Flash Player, Apple, Microsoft and Cisco. US-CERT also reported on recent and potential phishing scams.

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.

- NASA issued an advisory regarding a vulnerability in Common Data Format (CDF) versions 3.2 and earlier. This vulnerability is due to a buffer overflow condition in the handling of specially-crafted CDF files. Exploitation of this vulnerability may allow an attacker to execute arbitrary code.
- Microsoft released Windows XP Service Pack 3, which included multiple Hotfixes and security updates. In addition, Microsoft released its Security Bulletin for May 2008 that included updates to address multiple vulnerabilities in Microsoft Word, Publisher, and Jet Database Engine. These vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition.
- Cisco released multiple security advisories to address vulnerabilities in Cisco Unified Communications Manager, Unified Presence, Content Switching Module, IOS Secure Shell, Service Control Engine, Voice Portal, and CiscoWorks Common Services. These vulnerabilities

may allow an attacker to execute arbitrary code or cause a denial-of-service condition on the affected system.

- Debian and Ubuntu Linux operating systems released multiple security advisories to address vulnerabilities in their OpenSSL package and other cryptographic application packages that rely on it. Exploitation of these vulnerabilities may allow a remote, unauthenticated attacker to conduct brute force attacks and obtain sensitive information.
- Active exploitation of a vulnerability in Adobe Flash Player was reported. By convincing a user to open a specially crafted Flash file, which may be embedded in a compromised website, a remote, unauthenticated attacker may be able to execute arbitrary code.
- Apple released Mac OS X v10.5.3 and Security Update 2008-003 to address multiple vulnerabilities that affect a number of applications, libraries, and the kernel. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code, access the system with escalated privileges, obtain sensitive information, conduct cross-site scripting attacks, or cause a denial-of-service condition.

Current Activity for May 2008	
May 5	Common Data Format Buffer Overflow Vulnerability
May 6	PHP 5.2.6 Released
May 7	Microsoft Releases Windows XP Service Pack 3
May 8	Microsoft Releases Advance Notification for May Security Bulletin
May 9	Mozilla Releases Thunderbird 2.0.0.14
May 13	Microsoft Releases May Security Bulletin
May 14	Cisco Releases Security Advisories
May 15	Debian and Ubuntu OpenSSL and OpenSSH Vulnerabilities
May 15	United States Tax Court Spear-Phishing Attack
May 19	Natural Disasters and Phishing Scams
May 20	CA ARCserve Backup Vulnerabilities
May 22	Cisco Releases Security Advisories
May 22	IBM Lotus Sametime Vulnerability
May 27	Adobe Flash Player Vulnerability
May 28	Cisco Releases Security Advisory
May 29	Apple Releases Security Updates
May 29	Samba Releases Version 3.0.30

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 May 2008	
May 13	TA08-134A Microsoft Updates for Multiple Vulnerabilities
May 16	TA08-137A Debian/Ubuntu OpenSSL Random Number Generator Vulnerability
May 28	TA08-149A Exploitation of Adobe Flash Vulnerability
May 29	TA08-150A Apple 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 May 2008	
May 13	SA08-134A Microsoft Updates for Multiple Vulnerabilities
May 28	SA08-149A Exploitation of Adobe Flash Vulnerability
May 29	SA08-150A Apple 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 May 2008
SB08-126 Vulnerability Summary for the Week of April 28, 2008
SB08-133 Vulnerability Summary for the Week of May 5, 2008
SB08-140 Vulnerability Summary for the Week of May 12, 2008
SB08-147 Vulnerability Summary for the Week of May 19, 2008

A total of 384 vulnerabilities were recorded in the NVD during May 2008.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users and are issued every two weeks. May's tips focused on understanding website certificates and effective methods for erasing files.

Cyber Security Tips for May 2008	
May 14	ST05-010 Understanding Website Certificates
May 28	ST05-011 Effectively Erasing Files

Security Highlights

Phishing Scams Regarding Tax Season and Natural Disasters

In the month of May, US-CERT became aware of public reports regarding a spear phishing attack involving the US Tax Court and warned of potential phishing scams that may take advantage of the recent natural disasters.

The spear phishing attack circulated via email messages that claimed to be petitions from the US Tax Court. These messages appeared to be legitimate because they contained very specific information about the message recipient. The message requested that the user follow a link to download additional information about the petition, but if a user clicked on this link, malicious code may have been installed on the system. US-CERT encourages users to review the alert posted by the United States Tax Court regarding this issue.

In the past, US-CERT has received reports of an increased number of phishing scams following natural disasters. Due to the recent natural disasters (i.e., Myanmar cyclone, earthquakes in China), US-CERT would like to remind users to remain cautious when receiving unsolicited email that could be a potential phishing scam.

Phishing scams may appear as requests for donations from a charitable organization asking users to click on a link that will take them to a fraudulent website that appears to be a legitimate charity. The website may attempt to download malicious code. The users are then asked to provide personal information that can further expose them to future compromises.

US-CERT encourages users to review the Current Activity entry for more information regarding measures that can be taken to protect themselves from this type of phishing scam.

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