US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary

- October 2008 -

This report summarizes general activity as well as updates made to the National Cyber Alert System for the month of October. 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 October 2008, US-CERT issued 22 Current Activity entries, two (2) Technical Cyber Security Alerts, two (2) Cyber Security Alerts, four (4) weekly Cyber Security Bulletins, and three (3) Cyber Security Tips.

Highlights for this month include multiple updates released by VMware, Microsoft, Cisco, and Adobe; critical patches for Oracle and F-Secure products; phishing scams related to the financial crisis; and an update to the DNS cache poisoning vulnerability.

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.

- VMware released Security Advisory VMSA-2008-0016 to address multiple vulnerabilities. These vulnerabilities affect VMware hosted products, VirtualCenter, ESX, and ESXi. Exploitation of these vulnerabilities could allow an attacker to operate with escalated privileges in a guest operating system, obtain sensitive information, bypass security restrictions, or cause a denial-of-service condition.
- Microsoft released updates to address vulnerabilities in Microsoft Windows, Internet Explorer, Host Integration Server, and Office as part of the Microsoft Security Bulletin Summary for October 2008. These vulnerabilities could allow an attacker to execute arbitrary code, obtain sensitive information, or operate with elevated privileges.
- Microsoft also released an out-of-cycle Security Bulletin, MS08-067, to address a vulnerability in the Windows Server Service. This vulnerability exists due to improper handling of specially crafted RPC requests. Exploitation of this vulnerability could allow a remote attacker to execute

arbitrary code on a vulnerable system. Additionally, Microsoft released Security Advisory 958963 to address the release of publicly available exploit code.

- Cisco Security Advisory cisco-sa-20081008-unity was released to address a vulnerability in Cisco Unity, a voice and unified messaging platform. This vulnerability could allow an attacker to view and alter configuration parameters of the Cisco Unity server. This advisory was followed by Cisco Security Advisory cisco-sa-20081022-asa, which addressed multiple vulnerabilities in Cisco ASA and PIX that could allow an attacker to bypass authentication mechanisms or cause a denial-of-service condition.
- Adobe released Security Bulletin APSB08-18 to address multiple security issues in Flash Player. Some of these issues could allow an attacker to conduct Clickjacking types of attacks that could enable the camera or microphone through Flash Player. Adobe also released Security Advisory ASPA08-10 to address vulnerabilities in PageMaker 7.0.1 and 7.0.2. These vulnerabilities could allow an attacker to execute arbitrary code.
- Oracle released their Critical Patch Update for October 2008 to address 36 vulnerabilities across several products. This update contained security fixes for Oracle Database Suite, Oracle Application Server, Oracle E-Business Suite and Applications, Oracle PeopleSoft Enterprise, JD Edwards EnterpriseOne, and BEA Product Suite.
- F-Secure released Security Bulletin FSC-2008-3 to address a vulnerability that affects a number of their products across several platforms. This vulnerability is due to improper RPM parsing. Exploitation of this vulnerability may allow an attacker to execute arbitrary code.

Current Activity for October 2008	
October 6	Bank Acquisitions and Phishing Scams
October 6	VMware Security Advisory VMSA-2008-0016
October 6	Novell Releases eDirectory Version 8.7.3 SP10 FTF1
October 8	Cisco Releases Advisory for Cisco Unity
October 8	Opera Software Releases Opera Version 9.60
October 8	Multiple Web Browsers Affected by Clickjacking
October 9	Microsoft Releases Advance Notification for October Security Bulletin
October 10	CA ARCserve Backup Vulnerabilities
October 10	Apple Releases Security Update 2008-007
October 14	Microsoft Updates Security Advisory 951306
October 14	Microsoft Releases October Security Bulletin
October 15	Oracle Releases Critical Patch Update for October 2008
October 16	Adobe Releases Security Bulletin for Flash Player
October 21	F-Secure Releases Security Bulletin FSC-2008-3
October 22	Trend Micro OfficeScan Critical Patch Release
October 23	Cisco Releases Advisory for Cisco PIX and ASA
October 23	Microsoft Releases Advance Notification for Out-of-Band October Security Bulletin
October 27	Microsoft Releases Security Advisory 958963

Current Activity for October 2008	
October 27	Microsoft Releases Out-of-Band Security Bulletin MS08-067
October 29	OpenOffice.org Releases Two Security Bulletins
October 31	VMware Releases Security Advisory VMSA-2008-0017
October 31	Adobe Releases Security Advisory for PageMaker 7

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 October 2008	
October 14	TA08-288A Microsoft Updates for Multiple Vulnerabilities
October 23	TA08-297A Microsoft Windows Server Service RPC 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 October 2008	
October 14	SA08-288A Microsoft Updates for Multiple Vulnerabilities
October 23	SA08-297A Microsoft Windows Server Service 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 October 2008
SB08-280 Vulnerability Summary for the Week of September 29, 2008
SB08-287 Vulnerability Summary for the Week of October 6, 2008
SB08-294 Vulnerability Summary for the Week of October 13, 2008
SB08-301 Vulnerability Summary for the Week of October 20, 2008

A total of 535 vulnerabilities were recorded in the NVD during October 2008.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users and are issued every two weeks. September's tips focused on rootkits and botnets, debunking common myths, and online trading. Links to the full versions of these documents are listed below.

Cyber Security Tips for October 2008	
October 1	ST06-001 Understanding Hidden Threats: Rootkits and Botnets
October 15	ST06-002 Debunking Some Common Myths
October 29	ST06-004 Avoiding the Pitfalls of Online Trading

Security Highlights

Phishing Scams Take Advantage of Recent Financial News

US-CERT became aware of increases in public reports of phishing scams related to the current financial crisis. These phishing scams involve banks, savings and loan, or mortgage lenders that recently failed or were acquired by other institutions.

These scams may appear as requests for users to verify personal and bank account information, enroll in additional bank services, or activate new security features. Users should be wary of email messages or pop-up windows requesting this type of information. Messages may also contain a link that, when clicked, will take the user to a fraudulent website that closely resembles one from a legitimate financial institution. Users may be asked to provide personal and account information that can further expose them to future compromises. These fraudulent websites may also contain malicious code. Additional information can be found in FTC Consumer Alert ALT089.

US-CERT also reminds users to take the following measures to protect against phishing scams:

- Do not follow unsolicited web links received in email messages.
- Install anti-virus software, and keep its virus signature files up-to-date.
- Review the Recognizing and Avoiding Email Scams (pdf) document.
- Review the Avoiding Social Engineering and Phishing Attacks document.

Update to the DNS Cache Poisoning Vulnerability

In July 2008, US-CERT reported on a highly publicized vulnerability in which multiple DNS implementations were vulnerable to cache poisoning. DNS cache poisoning (sometimes referred to as cache pollution) is an attack technique that allows an attacker to introduce forged DNS information into the cache of a caching nameserver. An attacker with the ability to conduct a successful cache poisoning attack could cause a nameserver's clients to contact the incorrect, and possibly malicious, hosts for particular services. Consequently, web traffic, email, and other important network data could be redirected to systems under the attacker's control. Multiple vendors released patches to implement source port randomization in the nameserver to significantly reduce the practicality of cache poisoning attacks.

In August, the Internet System Consortium released updates for BIND 9.5.0-P2, BIND 9.4.2-P2, and BIND 9.3.5-P2, which included additional DNS security features to address this vulnerability.[1]

[1] http://www.us-cert.gov/current/archive/2008/08/14/archive.html#internet_system_consortium_releases_bind

Recently, a survey conducted by the network services provider Infoblox found that a significant number of DNS servers still remained vulnerable. Although 90% of those surveyed have implemented more secure versions of the BIND DNS software, about 40% still allow recursive queries, and 25% do not perform source port randomization. This indicates that a high proportion of servers remain vulnerable to cache poisoning and denial-of-service attacks.[2]

US-CERT reminds users to review "VU#800113 - Multiple DNS implementations vulnerable to cache poisoning" for solutions to help mitigate the risks and/or apply a vendor patch to vulnerable systems as soon as possible.

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

[2] http://www.gcn.com/online/vol1_no1/47524-1.html