US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary

- July 2008 -

This report summarizes general activity as well as updates made to the National Cyber Alert System for the month of July. 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 July 2008, US-CERT issued 25 current activity entries, four (4) technical cyber security alerts, two (2) cyber security alerts, four (4) weekly cyber security bulletin summary reports, and two (2) cyber security tips.

Highlights for this month include multiple security advisories released by Microsoft, Apple, Oracle, and Research in Motion (RIM); new versions of Mozilla Firefox; new Storm Worm activity, and the DNS cache poisoning vulnerability.

Contents

Current Activity

Current Activity entries 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.

- Microsoft released multiple security advisories to address various vulnerabilities in Windows, SQL Server, Windows Server Update Services, the Snapshot Viewer ActiveX control, and Word 2002 Service Pack 3.
- Apple released security updates to address multiple vulnerabilities in Mac OS X, Safari, iPhone, and iPod Touch.
- Oracle released its quarterly Critical Patch Update (CPU) in July to address 45 vulnerabilities across several products. In addition, Oracle released a security advisory detailing a vulnerability in the WebLogic plug-in for Apache that may allow a remote, unauthenticated attacker to compromise the confidentiality or integrity of WebLogic Server applications or cause a denial-of-service condition.
- Mozilla released three upgrades for the Firefox web browser. Versions 2.0.0.15, 2.0.0.16 and 3.0.1 addressed multiple vulnerabilities that could be exploited to allow a remote attacker to

conduct cross-site scripting attacks, upload arbitrary files, escalate privileges, execute arbitrary code, or cause a denial-of-service condition.

- RIM released a security advisory to address a vulnerability in the BlackBerry Enterprise Server. This vulnerability is due to the improper processing of PDF files within the distiller component of the BlackBerry Attachment Service, which may allow an attacker to execute arbitrary code on the system running the BlackBerry Attachment Service.
- US-CERT became aware of reports of new Storm Worm activity. The latest activity centered around email messages containing references to the conflict in the Middle East, the Federal Bureau of Investigation, and the social networking site Facebook.com. This Trojan is spread via unsolicited email messages that contain a link to a malicious website used to infect the user's system with malicious code.
- Details of deficiencies in the DNS protocol were publicly released. Implementations of this protocol may leave the affected system vulnerable to DNS cache poisoning attacks. A successful cache poisoning attack may cause a nameserver's clients to contact the incorrect, and possibly malicious, hosts for particular services. US-CERT released several current activity entries and a vulnerability note regarding this vulnerability. (See Security Highlights)

Current Activity for July 2008	
July 1	Apple Releases Security Updates
July 2	Mozilla Releases Firefox 2.0.0.15
July 3	Microsoft Releases Advanced Notification for July Security Bulletin
July 7	Microsoft Releases Security Advisory For Snapshot Viewer ActiveX Control
July 8	Microsoft Releases July Security Bulletin
July 9	New Storm Worm Variant Spreading
July 9	Microsoft Releases Security Advisory for Word Vulnerability
July 10	Sun Releases Updates for Java SE
July 11	Apple Releases Security Updates for iPhone and iPod touch
July 11	Oracle Critical Patch Update Pre-Release Announcement for July
July 14	Zone Alarm Releases Security Advisory
July 15	Oracle Releases Critical Patch Update for July 2008
July 16	WordPress Releases Version 2.6
July 16	Mozilla Releases Firefox 2.0.0.16
July 17	Mozilla Releases Firefox 3.0.1
July 18	BlackBerry Security Advisory
July 22	DNS Implementations Vulnerable to Cache Poisoning
July 23	NAT/PAT Affects DNS Cache Poisoning Mitigation
July 24	DNS Cache Poisoning Public Exploit Code Available
July 25	U.S. Customs and Border Protection Email Attack
July 28	RealPlayer Releases Update

Current Activity for July 2008	
July 29	Oracle Releases Security Advisory for WebLogic Plug-in Vulnerability
July 29	New Storm Worm Activity Spreading
July 31	AVG Releases Update
July 31	Airline E-ticket Email Attack

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 July 2008	
July 7	TA08-189A Microsoft Office Snapshot Viewer ActiveX Vulnerability
July 8	TA08-190A Microsoft Updates for Multiple Vulnerabilities
July 8	TA08-190B Multiple DNS implementations vulnerable to cache poisoning
July 11	TA08-193A Sun Java 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 July 2008	
July 8	SA08-190A Microsoft Updates for Multiple Vulnerabilities
July 11	SA08-193A Sun 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 July 2008
SB08-189 Vulnerability Summary for the Week of June 30, 2008
SB08-196 Vulnerability Summary for the Week of July 7, 2008
SB08-203 Vulnerability Summary for the Week of July 14, 2008
SB08-210 Vulnerability Summary for the Week of July 21, 2008

A total of 519 vulnerabilities were recorded in the NVD during July 2008.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users and are issued every two weeks. July's tips focused on online safety and understanding Bluetooth technology.

Cyber Security Tips for July 2008	
July 9	ST05-014 - Real-World Warnings Keep You Safe Online
June 23	ST05-015 - Understanding Bluetooth Technology

Security Highlights

DNS Cache Poisoning

DNS servers employ caches of memory to improve their performance when answering multiple identical queries. When a DNS server answers a query with information that did not originate from an authoritative DNS server, it is considered poisoned. 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. Due to the caching mechanism, a poisoned DNS server will continue to answer queries for the forged information until the cached answer times out.

US-CERT first reported on this on July 8, when multiple vendors released updates to resolve weakness in DNS implementations that could leave vulnerable systems open to cache poisoning. These patches implement source port randomization in the nameserver as a way to reduce the practicality of cache poisoning attacks. US-CERT released Vulnerability Note VU#800113 and a Current Activity entry to detail the vulnerability and provide mitigation strategies.

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