US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary

- June 2008 -

This report summarizes general activity as well as updates made to the National Cyber Alert System for the month of June. 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 June 2008, US-CERT issued 21 current activity entries, three (3) technical cyber security alerts, two (2) cyber security alerts, five (5) weekly cyber security bulletin summary reports, and two (2) cyber security tips.

Highlights for this month include multiple advisories from Microsoft and Cisco, updates from Apple, Microsoft, and Adobe, new phishing activity linked to Storm Worm, a vulnerability regarding SNMP version 3, and multiple web browser vulnerabilities.

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 in June:
  - Security Advisory 953818 addressed reports of a blended threat affecting Windows users who installed Apple's Safari web browser.
  - Security Advisory 954462 was issued in response to a recent increase in SQL injection attacks targeting websites using Microsoft ASP and ASP.NET.
  - Security Advisory 954960 was issued regarding a failure by Microsoft Windows Server Update Services to properly deploy updates within certain environments.
- Microsoft released its June 2008 Security Bulletin to address vulnerabilities in Windows and Internet Explorer. Later in the month, Microsoft released an update to security bulletin MS08-030 to address a critical vulnerability in the Bluetooth stack for Windows.
- Cisco released a security advisory to address multiple vulnerabilities in Cisco PIX and ASA security appliances that could allow an attacker to cause a denial of service condition or bypass

security restrictions. Additionally, Cisco released an advisory to address a vulnerability in several of its Intrusion Prevention System platforms. Exploitation of this vulnerability could allow a remote attacker to trigger a kernel panic and cause a denial-of-service condition or bypass security restrictions.

- Apple released QuickTime 7.5 to address multiple vulnerabilities that could allow a remote attacker to execute arbitrary code or cause a denial-of-service condition. Additionally, Apple released Safari v3.1.2 for Windows to address multiple vulnerabilities that could lead to the disclosure of memory contents, arbitrary code execution, or unexpected application termination.
- US-CERT received reports of new phishing activity, some of which has been linked to Storm Worm. The latest activity was centered around messages related to the recent earthquake in China and the upcoming Olympic Games. This Trojan is spread via an unsolicited email message that contains a link to a malicious website.
- Adobe released a security update for Adobe Reader and Acrobat version 8.1.2 to address a vulnerability that may allow a remote attacker to execute arbitrary code or cause a denial-of-service condition.
- US-CERT became aware of a vulnerability in implementations of SNMP version 3. This vulnerability is due to an error in the way the authenticator field handles a shortened hash message authentication code (HMAC). Exploitation of this vulnerability may allow an attacker to read and modify any SNMP object or the configuration of the affected device.

Current Activity for June 2008	
June 2	Microsoft Releases Security Advisory
June 2	VMware Releases Security Advisory
June 4	HP Instant Support ActiveX Control Vulnerabilities
June 4	Sun Releases Java ASP Server 4.0.3
June 4	United States Tax Court Phishing Attack
June 5	Microsoft Releases Advance Notification for June Security Bulletin
June 5	Skype Releases Security Bulletin
June 5	Cisco Releases Security Advisory
June 10	Microsoft Releases June Security Bulletin
June 10	SNMPv3 Authentication Bypass Vulnerability
June 10	Apple Releases QuickTime 7.5
June 19	New Phishing/Storm Worm Variant Spreading
June 19	Cisco Releases Security Advisory
June 20	Critical Vulnerability in Microsoft Bluetooth Stack
June 20	Apple Releases Safari v3.1.2 for Windows
June 24	Microsoft Releases Security Advisory
June 24	Adobe Releases Security Bulletin
June 26	Microsoft Internet Explorer 6 Cross-Domain Vulnerability
June 27	Microsoft Internet Explorer Frame Vulnerability
June 30	Cisco Releases Security Advisory

Current Activity for June 2008	
June 30	Microsoft Releases Security Advisory

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 June 2008	
June 10	TA08-162A SNMPv3 Authentication Bypass Vulnerability
June 10	TA08-162B Microsoft Updates for Multiple Vulnerabilities
June 10	TA08-162C Apple QuickTime 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 June 2008	
June 10	SA08-162B Microsoft Updates for Multiple Vulnerabilities
June 10	SA08-162C Apple QuickTime 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 June 2008
SB08-154 Vulnerability Summary for the Week of May 26, 2008
SB08-161 Vulnerability Summary for the Week of June 2, 2008
SB08-168 Vulnerability Summary for the Week of June 9, 2008
SB08-175 Vulnerability Summary for the Week of June 16, 2008
SB08-182 Vulnerability Summary for the Week of June 23, 2008

A total of 435 vulnerabilities were recorded in the NVD during June 2008.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users and are issued every two weeks. June's tips focused on supplementing passwords and guidelines for publishing information online. Links to the full versions of these documents are listed below.

Cyber Security Tips for June 2008	
June 11	ST05-012 Supplementing Passwords
June 26	ST05-013 Guidelines for Publishing Information Online

Security Highlights

Multiple vulnerabilities were reported in Microsoft Internet Explorer and Apple Safari for Windows in the month of June. Publicly available proof-of-concept code for a vulnerability affecting Microsoft Internet Explorer 6, 7, and 8 beta 1 was reported. This vulnerability is due to improper access restriction to certain components of a document's frames. Exploitation of this vulnerability could allow an attacker to capture keystrokes or perform other malicious acts. Additional information can be found in US-CERT Vulnerability Note VU#516627.

US-CERT also received reports of a cross-domain vulnerability in Internet Explorer 6 with publicly available proof-of-concept code. By convincing a user to view a specially crafted HTML document (e.g., a web page or an HTML email message), an attacker may be able to obtain access to web content in another domain. Additional information about this vulnerability can be found in US-CERT Vulnerability Note VU#923508.

Apple released Safari v3.1.2 for Windows to address multiple vulnerabilities that included:

- an out-of-bounds memory read when handling BMP and GIF files that may lead to the disclosure of memory contents
- an issue in the way Windows desktop handles executables, which may allow arbitrary code execution
- an issue in the way Safari handles executables from websites in a trusted Internet Explorer zone, which may lead to automatic arbitrary code execution
- a memory corruption issue in the handling of JavaScript arrays by WebKit that may lead to an unexpected application termination or arbitrary code execution

Additional details are provided in Apple Article HT2092.

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