US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary

- April 2008 -

This report summarizes general activity as well as updates made to the National Cyber Alert System for the month of April. 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 April 2008, US-CERT issued 28 current activity entries, three (3) technical cyber security alerts, three (3) cyber security alerts, four (4) weekly cyber security bulletin summary reports, and three (3) cyber security tips.

Highlights for this month include updates for Microsoft, Apple, Oracle, various web browsers and multimedia players. US-CERT also reported on compromised websites hosting malicious JavaScript.

Contents

Executive Summary……1

Current Activity……1

Technical Cyber Security Alerts……2

Cyber Security Alerts……3

Cyber Security Bulletins……3

Cyber Security Tips……4

Security Highlights……4

Contacting US-CERT……4

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.

- Apple issued updates for several vulnerabilities in Safari web browser and QuickTime multimedia player. Exploitation of these vulnerabilities may result in execution of arbitrary code, information disclosure, denial of service, or cross-site scripting attacks.
- Microsoft's April security bulletin contained updates to address multiple vulnerabilities in Microsoft Windows, Office, Internet Explorer, Project, and Visio. These vulnerabilities could result in remote code execution, escalation of privileges or redirection of internet traffic.
- Mozilla Firefox and Opera released updates to address multiple vulnerabilities. Firefox 2.0.0.14 addressed memory corruption errors in the JavaScript engine. Opera 9.27 included fixes for errors in adding newsfeeds and issues in the processing of HTML CANVAS elements that could lead to arbitrary code execution or denial-of-service conditions.
- Oracle released a Critical Patch Update for April to address 41 vulnerabilities across several products including Oracle Database, Enterprise Manager, E-Business Suite, PeopleSoft Enterprise, and Siebel SimBuilder.

- SQL injection attacks were reported to have compromised a large number of legitimate websites with JavaScript code that exploited multiple, known vulnerabilities. Users with vulnerable systems who visited the infected websites may have unknowingly executed malicious code.

Current Activity for April 2008	
April 1	PayPal Phishing Attack
April 1	Macrovision InstallShield ActiveX Vulnerability
April 3	Microsoft Releases Advance Notification for April Security Bulletin
April 3	Opera 9.27 Released
April 3	Apple Releases QuickTime 7.4.5
April 4	RealPlayer Update Released
April 4	CA BrightStor ARCserve Backup Vulnerabilities
April 4	Cisco Unified Communication Disaster Recovery Framework Vulnerability
April 7	Email Attack Targeting Microsoft's April Security Bulletin Release Cycle
April 8	Microsoft Releases April Security Bulletin
April 9	Email Attack Circulating
April 9	Adobe Flash Player Vulnerabilities
April 9	IBM Lotus Notes Vulnerabilities
April 11	Active Exploitation of GDI Vulnerabilities
April 14	Oracle Issues Pre-Release Announcement for April Critical Patch Update
April 14	EMC DiskXtender Vulnerabilities
April 15	Oracle Releases Critical Patch Update for April 2008
April 15	Multiple ClamAV Vulnerabilities
April 16	Federal Subpoena Spear-Phishing Attack
April 17	Apple Releases Safari 3.1.1
April 17	Mozilla Releases Firefox 2.0.0.14
April 18	Microsoft Releases Security Advisory (951306)
April 22	ICQ Vulnerability
April 23	Apple QuickTime Vulnerability Report
April 24	IRS Rebate Phishing Scam
April 25	Compromised Websites Hosting Malicious JavaScript
April 25	HP Software Update Vulnerabilities
April 28	WordPress Vulnerabilities

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 April 2008	
April 3	TA08-094A Apple Updates for Multiple Vulnerabilities
April 8	TA08-099A Microsoft Updates for Multiple Vulnerabilities
April 9	TA08-100A Adobe Flash 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 April 2008	
April 3	SA08-094A Apple QuickTime Updates for Multiple Vulnerabilities
April 8	SA08-099A Microsoft Updates for Multiple Vulnerabilities
April 9	SA08-100A 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 April 2008
SB08-098 Vulnerability Summary for the Week of March 31, 2008
SB08-105 Vulnerability Summary for the Week of April 7, 2008
SB08-112 Vulnerability Summary for the Week of April 14, 2008
SB08-119 Vulnerability Summary for the Week of April 21, 2008

A total of 455 vulnerabilities were recorded in the NVD during April 2008.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users and are issued every two weeks. April's tips focused on the risks of file-sharing, online anonymity, and free email services.

Cyber Security Tips for April 2008	
April 3	ST05-007 Risks of File-Sharing Technology
April 17	ST05-008 How Anonymous Are You?
April 30	ST05-009 Benefits and Risks of Free Email Services

Security Highlights

Massive Web Compromises

In late April, US-CERT published a current activity update to warn users of SQL injection attacks that had compromised thousands of web pages. The compromised web pages contained injected JavaScript that attempted to exploit multiple, known vulnerabilities. Users who visited a compromised website may have unknowingly executed malicious code.

It's important to note that some of the affected web pages have since been sanitized. However, it's likely that many are still affected and hosting malicious code. US-CERT recommends maintaining up to date patches and disabling JavaScript and ActiveX as described in the Securing Your Web Browser document.

Multimedia Player Vulnerabilities

Several widely used multimedia player vendors released updates for multiple vulnerabilities, including QuickTime, RealPlayer, and Adobe Flash Player.

- Apple has released Apple QuickTime 7.4.5 to correct several vulnerabilities as described in Apple Knowledgebase article HT1241. Additional details are described in the Cyber Security Alert SA08-094A.
- RealNetworks released an update to address an ActiveX vulnerability. Refer to vulnerability note VU#831457 for additional details.
- Adobe has released Security advisory APSB08-11 to address multiple vulnerabilities affecting Adobe Flash. Details can be found in Technical Cyber Security Alert TA08-100A.

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