US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary

- June 2012 -

This report summarizes general activity including updates to the National Cyber Awareness System in June 2012. It includes current activity updates, alerts, and bulletins, in addition to other newsworthy events or highlights.

Executive Summary

During June 2012, US-CERT issued 13 Current Activity entries, three Alerts, and four weekly Bulletins.

Highlights for this month include updates or advisories released by Microsoft, Adobe, Oracle, Google, and Apple.

Contents

Current Activity

Current Activity entries are high-impact security threats and vulnerabilities currently reported to US-CERT. The following table lists all of the entries posted this month followed by a brief overview of the most significant entries.

Current Activity for June 2012	
June 4	Unauthorized Microsoft Digital Certificates
June 5	Adobe Releases Security Bulletins for Multiple Products
June 6	Mozilla Releases Multiple Updates
June 7	Microsoft Releases Advance Notification for June Security Bulletin
June 11	Adobe Releases Security Bulletin for Adobe Flash Player
June 12	Apple Releases iTunes 10.6.3
June 12	Microsoft Releases June Security Bulletin
June 13	Oracle Releases Critical Patch Update for June 2012
June 13	Microsoft Releases Security Advisory for Microsoft XML Core Services
June 14	Apple Releases Java Update for OS X Lion and Mac OS X
June 21	Cisco Releases Multiple Security Advisories
June 27	Google Releases Google Chrome 20.0.1132.43
June 29	Cisco Releases Security Advisory for WebEx Player

- Microsoft released its monthly Security Bulletin and several Security Advisories:
  - Microsoft released updates to address vulnerabilities in Microsoft Windows, Internet Explorer, .NET Framework, Lync, and Dynamics AX as part of the Microsoft Security Bulletin Summary for June 2012. These vulnerabilities may allow an attacker to execute arbitrary code or operate with elevated privileges. Additional information regarding CVE-2012-0217 can be found in the US-CERT Vulnerability Note VU#649219.
  - Security advisory 2718704 addressed the revocation of a number of unauthorized digital certificates. Maintaining these certificates within your certificate store may allow an attacker to spoof content, perform a phishing attack, or perform a man-in-the-middle attack. Two Microsoft Enforced Licensing Intermediate PCA certificates and a Microsoft Enforced Licensing Registration Authority CA SHA1 certificate were revoked by this update. Microsoft provided an update to all support versions of Microsoft Windows to address this issue.
  - Security Advisory 2719615 addressed a vulnerability in Microsoft XML Core Services 3.0, 4.0, 5.0, and 6.0. This vulnerability may allow an attacker to execute arbitrary code if a user accesses specially crafted web pages using Internet Explorer. According to the advisory, this vulnerability is currently being exploited in the wild.
- Google released Google Chrome 20.0.1132.43 for Linux, Mac, Windows, and Chrome Frame to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition.
- Adobe released security bulletins to address multiple vulnerabilities in Adobe Illustrator CS5 (15.0.x) for Windows and Macintosh, Adobe Illustrator CS5.5 (15.1) for Windows and Macintosh, Adobe Photoshop CS5 (12.0) for Windows and Macintosh, and Adobe Photoshop CS5.1 (12.1) for Windows and Macintosh. Adobe also released a Security Bulletin for Adobe Flash Player to address vulnerabilities affecting Adobe Flash Player 11.2.202.235 and earlier versions for Windows, Macintosh, and Linux; Adobe Flash Player 11.1.115.8 and earlier versions for Android 4.x, Adobe Flash Player 11.1.111.9 and earlier versions for Android 3.x and 2.x. These vulnerabilities may allow an attacker to take control of the affected system or cause a denial-of-service condition.
- Apple released a Java update to address multiple vulnerabilities in Mac OS X v10.6.8, Mac OS X Server v10.6.8, OS X Lion v10.7.4, and OS X Lion Server v10.7.4. These vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition. Apple also released iTunes 10.6.3 to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition.
- Oracle released its Critical Patch Update for June 2012 containing 14 security fixes for JDK and JRE 7 Updates 4 and earlier, JDK and JRE 6 Update 32 and earlier, JDK and JRE 5.0 Update 35 and earlier, SDK and JRE 1.4.2_37 and earlier, and JavaFX 2.1 and earlier.
- The Mozilla Foundation released updates to address multiple vulnerabilities in Firefox 13.0, Firefox ESR 10.0.5, Thunderbird 13.0, Thunderbird ESR 10.0.5, and SeaMonkey 2.10. These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, disclose sensitive information, operate with elevated privileges, or perform a cross-site scripting attack.
- Cisco released three security advisories to address vulnerabilities affecting Cisco ASA 5500 Series Adaptive Security Appliances (Cisco ASA), Cisco Catalyst 6500 Series ASA Service Module (Cisco ASASM), Cisco AnyConnect Secure Mobility Client, and Cisco Application Control Engine (ACE). These vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition. Cisco also released a security advisory to address vulnerabilities affecting Cisco WebEx Recording Format (WRF) and Cisco Advanced Recording

Format (ARF). These vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition. US-CERT encourages users and administrators to review Cisco Security Advisories cisco-sa-20120620-asaipv6, cisco-sa-20120620-ac, cisco-sa-20120620-ace, and cisco-sa-20120627-webex and apply any necessary updates to help mitigate this risks.

Alerts

Alerts provide timely information about current security issues, vulnerabilities, and exploits.

Alerts for June 2012	
June 4	TA12-156A Microsoft Windows Unauthorized Digital Certificates
June 12	TA12-164A Microsoft Updates for Multiple Vulnerabilities
June 22	TA12-174A Microsoft XML Core Services Attack Activity

Bulletins

Bulletins are issued weekly and provide a summary of new vulnerabilities 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)/US-CERT. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

Bulletins for June 2012	
June 4	SB12-156 Vulnerability Summary for the Week of May 28, 2012
June 11	SB12-163 Vulnerability Summary for the Week of June 4, 2012
June 18	SB12-170 Vulnerability Summary for the Week of June 11, 2012
June 25	SB12-177 Vulnerability Summary for the Week of June 18, 2012

A total of 406 vulnerabilities were recorded in the NVD during June 2012.

Security Highlights

Unauthorized Microsoft Digital Certificates

Microsoft has released a security advisory to address the revocation of a number of unauthorized digital certificates. Maintaining these certificates within your certificate store may allow an attacker to spoof content, perform a phishing attack, or perform a man-in-the-middle attack.

The following certificates have been revoked by this update:

- Microsoft Enforced Licensing Intermediate PCA (two certificates)
- Microsoft Enforced Licensing Registration Authority CA (SHA1)

Microsoft has provided an update to all support versions of Microsoft Windows to address this issue. Additional information can be found in Microsoft Security Advisory 2718704.

US-CERT encourages users and administrators to apply any necessary updates to help mitigate the risk.

Contacting US-CERT

If you would like to contact US-CERT to ask a question, submit an incident, or learn more about cybersecurity, 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: 0xEDA10949
PGP Key Fingerprint: 5A24 6040 50FC 1BA3 81FA 0919 1378 C036 EDA1 0949
PGP Key: https://www.us-cert.gov/pgp/info.asc