US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary
- September 2010 -

This report summarizes general activity as well as updates made to the National Cyber Alert System in September 2010. It 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 September 2010, US-CERT issued 12 Current Activity entries, two Technical Cyber Security Alerts, one Cyber Security Alert, four weekly Cyber Security Bulletins, and two Cyber Security Tips.

Highlights for this month include updates released by Microsoft, Oracle, Cisco, Apple, Google, and Mozilla; the Windows .LNK vulnerability; and a malicious email campaign.

Contents

Executive Summary……1

Current Activity……1

Technical Cyber Security Alerts……3

Cyber Security Alerts……4

Cyber Security Bulletins……4

Cyber Security Tips……4

Security Highlights……4

Contacting US-CERT……5

Current Activity

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

Current Activity for September 2010	
September 1	VMware Releases Updates for ESX Service Console Packages
September 1	Insecure Loading of Dynamic Link Libraries in Windows Applications
September 3	Google Releases Chrome 6.0.472.53
September 3	Apple Releases iTunes 10
September 8	Apple Releases Safari 5.0.2 and 4.1.2
September 8	Mozilla Releases Firefox 3.6.9
September 9	Cisco Releases Updates for Wireless LAN Controller
September 9	Microsoft Releases Advance Notification for September Security Bulletin
September 9	Malicious Email Campaign Circulating
September 10	Insecure Loading of Dynamic Link Libraries in Windows Applications

Current Activity for September 2010	
September 13	Adobe Releases Security Advisory for Vulnerability in Reader and Acrobat
September 14	Adobe Releases Security Advisory for Flash Player
September 14	Microsoft Releases September Security Bulletin
September 15	Google Releases Chrome 6.0.472.59
September 16	Insecure Loading of Dynamic Link Libraries in Windows Applications
September 16	Apple Releases QuickTime 7.6.8
September 16	Mozilla Releases Firefox 3.5.13 and 3.6.10
September 20	Adobe Releases Security Advisory for Flash Player
September 20	Microsoft Releases Security Advisory 2416728
September 21	Apple Releases Security Update 2010-006
September 23	Cisco Releases Security Advisories
September 23	OpenX Releases Security Update
September 27	Microsoft Releases Security Advisory 2416728
September 28	Microsoft Releases Advance Notification for Out-of-Band Security Bulletin
September 28	Microsoft Releases Security Bulletin MS10-070

- Adobe addressed multiple vulnerabilities in Acrobat, Reader, and Flash Player:
  - Security Advisory APSA10-02 addressed an actively exploited vulnerability in Adobe Reader and Acrobat. Exploitation of this vulnerability may allow an attacker to execute arbitrary code or cause a denial-of-service condition.
  - Security Advisory APSA10-03 alerted users to a vulnerability affecting Adobe Flash Player. This vulnerability affects Flash Player 10.1.82.76 and earlier versions for Windows, Macintosh, Linux, Solaris, and Adobe Flash Player 10.1.92.10 for Android. Exploitation of this vulnerability may allow an attacker to execute arbitrary code or cause a denial-of-service condition.
- Apple addressed multiple vulnerabilities with update releases:
  - iTunes 10 addressed vulnerabilities affecting the WebKit package, and Safari 5.0.2 and 4.1.2 addressed vulnerabilities in the Safari and WebKit packages. These vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition.
  - Security Update 2010-006 for Mac OS X and Mac OS X Server addressed a vulnerability in the AFP package; if exploited, the vulnerability may allow an attacker to bypass password validation and obtain sensitive information.
- Cisco addressed vulnerabilities affecting Cisco Wireless LAN and Cisco IOS software:
  - Cisco security advisory provides updates to Cisco Wireless LAN Controller (WLC) and addressed vulnerabilities that may allow a remote attacker to cause a denial-of-service condition, modify the device configuration, or bypass access control lists.
  - Six security advisories addressed vulnerabilities affecting the Cisco IOS Software and the Cisco Unified Communications Manager. Exploitation of these vulnerabilities may allow an attacker to cause a denial-of-service condition. Users are encouraged to review the following:

- Cisco IOS Software H.323 Denial of Service Vulnerabilities
- Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerabilities
- Cisco IOS Software Internet Group Management Protocol Denial of Service Vulnerability
- Cisco IOS Software Network Address Translation Vulnerabilities
- Cisco IOS SSL VPN Vulnerability
- Cisco Unified Communication Manager Session Initiation Protocol Denial of Service Vulnerabilities

- Google released two updates for Chrome web browser. Versions 6.0.472.53 and 6.0.472.59 were released for Linux, Mac, and Windows to address multiple vulnerabilities that could allow an attacker to execute arbitrary code.
- Microsoft released security advisories, updates, and bulletins:
  - Security Bulletin MS10-070 addressed a vulnerability affecting ASP.NET that may allow an attacker to obtain sensitive information or tamper with data.
  - Security Advisory 2416728 alerted users of a vulnerability affecting ASP.NET that may allow an attacker to obtain sensitive information or tamper with data. This vulnerability affected all applications that rely on the ASP.NET platform.
- Mozilla released multiple updates for the Firefox web browser. Firefox 3.6.9 addressed multiple vulnerabilities that may allow an attacker to execute arbitrary code, obtain sensitive information, leverage cross-site scripting attacks, or cause a denial-of-service condition. Firefox 3.5.12 addressed these same vulnerabilities, many of which also affect Thunderbird and SeaMonkey. Firefox 3.5.13 and 3.6.10 addressed a stability issue affecting some users.
- OpenX released a security update to address a vulnerability in the 2.8 downloadable version of its advertising software. Exploitation of this vulnerability may allow an attacker to compromise the integrity of the server running OpenX.
- VMware released security updates for multiple third party packages for the ESX Service Console. These updates address vulnerabilities in the Perl, Kerberos release 5 (krb5), Samba, tarball (.tar), and Copy In and Out (.cpio) packages. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, or bypass security restrictions.
- Apple, Research In Motion (RIM), and Microsoft released fixes for Insecure Loading of Dynamic Link Libraries (DLL) in Windows Applications:
  - Apple released QuickTime 7.6.8 to address the DLL issue in earlier versions of Quicktime for Windows.
  - RIM released a security advisory to address the DLL issue in its BlackBerry Desktop Software for Windows version 6.0. This issue impacts all versions of the BlackBerry Desktop Software and may allow an attacker to convince the user to execute arbitrary code.
  - Microsoft released Fix it tool 50522 to assist users in setting the registry key value introduced with Microsoft support article 2264107 to help reduce the risks posed by the DLL loading behavior described in VU#707943.

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 September 2010	
September 14	TA10-257A Microsoft Updates for Multiple Vulnerabilities
September 20	TA10-263A Adobe Flash 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 September 2010	
September 14	SA10-257A Microsoft Updates for Multiple Vulnerabilities
September 20	SA10-263A Adobe Flash Vulnerabilities

Cyber Security Bulletins

Cyber Security Bulletins are issued weekly and provide a summary of new vulnerabilities recorded by the National Institute of Standards and Technology's (NIST's) 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.

Security Bulletins for September 2010
SB10-249 Vulnerability Summary for the Week of August 30, 2010
SB10-256 Vulnerability Summary for the Week of September 6, 2010
SB10-263 Vulnerability Summary for the Week of September 13, 2010
SB10-270 Vulnerability Summary for the Week of September 20, 2010

A total of 297 vulnerabilities were recorded in the NVD during September 2010.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users. The September tips focused on end-user license agreements and file-sharing technology.

Cyber Security Tips for September 2010	
September 8	ST05-015 Understanding Bluetooth Technology
September 29	ST05-017 Cybersecurity for Electronic Devices

Security Highlights

Microsoft Windows .LNK Vulnerability

A vulnerability exists in Microsoft Windows due to the failure of the operating system to properly obtain icons for .LNK files. Microsoft uses .LNK files, commonly referred to as "shortcuts," as references to files or applications.

By convincing a user to display a specially crafted .LNK file, an attacker could execute arbitrary code that would give the attacker the privileges of the user. Viewing the location of an .LNK file with Windows Explorer is sufficient to trigger the vulnerability. By default, Microsoft Windows is configured with the AutoRun/AutoPlay features enabled. These features can cause Windows to automatically open Windows Explorer when a removable drive is connected, thus opening the location of the .LNK and triggering the vulnerability. Other applications that display file icons can be used as an attack vector for this vulnerability as well. Depending on the operating system and AutoRun/AutoPlay configuration, exploitation can occur without any interaction from the user. This vulnerability can also be exploited remotely through a malicious website, through a malicious file, or WebDAV share.

Microsoft released Security Advisory 2286198 in September to provide mitigation steps. US-CERT also provided the following best practice security measures to help further reduce the risks of this and other vulnerabilities:

- Disable AutoRun as described in Microsoft Support article 967715.
- Implement the principle of least privilege as defined in the Microsoft TechNet Library.
- Maintain up-to-date antivirus software.
- Additional information can be found in the US-CERT Vulnerability Note VU#940193.

Malicious Email Campaign Circulated

In September 2010, multiple organizations across the public and private sectors were impacted by malware spreading via email. The public reports indicated that the malicious messages contained the subject line "Here you have" or "Just For You" and included a link to a seemingly legitimate PDF file. Users who clicked on this link were redirected to a malicious website that prompted them to download and install a screensaver (.scr) file. Users who agreed to install this file became infected with an email worm that propagated through their email contacts.

US-CERT encourages users and administrators to take the following preventive measures to help mitigate the security risks:

- Install antivirus software, and keep its virus signature files up-to-date.
- Do not follow unsolicited web links received in email messages.
- Refer to the Recognizing and Avoiding Email Scams (PDF) document for more information on avoiding email scams.
- Refer to the Avoiding Social Engineering and Phishing Attacks document for more information on avoiding social engineering and phishing attacks.

Contacting US-CERT

If you would like to contact US-CERT to ask a question, submit an incident, or 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 e-mail info@us-cert.gov.

Web Site Address: http://www.us-cert.gov
E-mail Address: info@us-cert.gov
Phone Number: +1 (888) 282-0870
PGP Key ID: 0x91D70D64
PGP Key Fingerprint: EAAC 46A4 4CEC 8A78 EED2 73F3 E5F3 5D6C 91D7 0D64
PGP Key: https://www.us-cert.gov/pgp/info.asc