US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary
- July 2010 -

This report summarizes general activity as well as updates made to the National Cyber Alert System in July 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 July 2010, US-CERT issued 12 Current Activity entries, 2 Technical Cyber Security Alerts, 1 Cyber Security Alert, 4 weekly Cyber Security Bulletins, and 2 Cyber Security Tips.

Highlights for this month include updates released by Microsoft, Oracle, Cisco, Apple, Google, and Mozilla.

Contents

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 July 2010	
July 7	Google Releases Chrome 5.0.375.99
July 8	Microsoft Releases Advance Notification for July Security Bulletin
July 9	Oracle Critical Patch Update Pre-Release Announcement
July 13	Oracle Releases Critical Patch Update for July 2010
July 13	Microsoft Releases July Security Bulletin
July 20	Apple Releases iTunes 9.2.1
July 21	Mozilla Releases Firefox 3.6.7
July 21	Microsoft Windows .LNK Vulnerability
July 22	Cisco Releases Security Advisory for CDS Internet Streamer
July 26	Firefox Releases Firefox 3.6.8

Current Activity for July 2010	
July 27	Google Releases Chrome 5.0.375.125
July 28	Apple Releases Safari 5.0.1 and Safari 4.1.1
July 30	Microsoft Windows .LNK Vulnerability

- Microsoft released updates to address vulnerabilities in Microsoft Windows and Office as part of the Microsoft Security Bulletin Summary for July 2010. These vulnerabilities may allow an attacker to execute arbitrary code in multiple versions of Microsoft Windows and Office.
- Oracle released its Critical Patch Update for July 2010 to address 59 vulnerabilities across multiple products such as Oracle Database Server; TimesTen In-Memory Database; Oracle Secure Backup; Oracle Fusion Middleware; Oracle Enterprise Manager; Oracle E-Business Suite; Oracle Supply Chain Products Suite; Oracle PeopleSoft and JD Edwards Suite; and Oracle Sun Products Suite.
- Cisco released security advisory cisco-sa-20100721 to address a vulnerability in the Cisco Internet Streamer application that is part of the Cisco Content Delivery System. Exploitation of this vulnerability may allow a remote, unauthenticated attacker to obtain sensitive information, including password files and system logs. This information could be used to leverage subsequent attacks.
- Apple released updates for iTunes and Safari.
  - The release of iTunes 9.2.1 addressed a vulnerability due to improper handling of the ITPC protocol used by iTunes for handling podcasts. By convincing a user to access a specially crafted ITPC URL, an attacker could execute arbitrary code or cause a denial-of-service condition. Additional details are described in Apple article HT4263.
  - Safari 5.0.1 and Safari 4.1.1 for Windows and Mac OS X addressed multiple vulnerabilities in Safari and WebKit. These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, or obtain sensitive information. Refer to Apple article HT4276 for additional details.
- Google released two updates for its Chrome web browser. Chrome 5.0.375.125 for Linux, Mac, and Windows addressed multiple vulnerabilities that could allow an attacker to execute arbitrary code or obtain sensitive information. Later in July, Google released Chrome 5.0.375.99 for Linux, Mac, and Windows to address multiple vulnerabilities that may allow an attacker to execute arbitrary code or cause a denial-of-service condition. Release details are provided in the Google Chrome blog entry.
- The Mozilla Foundation released Firefox 3.6.8 to address a critical vulnerability as described in security advisory MFSA 2010-48. This vulnerability may allow an attacker to execute arbitrary code. Previous releases in July included Firefox 3.6.7 and Firefox 3.5.11, which addressed multiple vulnerabilities that could allow an attacker to execute arbitrary code, obtain sensitive information, bypass security restrictions, or conduct cross-site scripting attacks. Some of these vulnerabilities also affected Thunderbird and SeaMonkey. Additional information can be found in the Mozilla Foundation security advisories released on July 20, 2010.

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 2010	
July 13	TA10-194B Oracle Updates for Multiple Vulnerabilities
July 13	TA10-194A Microsoft 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 2010	
July 13	SA10-194A Microsoft Updates for Multiple 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 July 2010
SB10-186 Vulnerability Summary for the Week of June 28, 2010
SB10-193 Vulnerability Summary for the Week of July 5, 2010
SB10-200 Vulnerability Summary for the Week of July 12, 2010
SB10-207 Vulnerability Summary for the Week of July 19, 2010

A total of 343 vulnerabilities were recorded in the NVD during July 2010.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users.

Cyber Security Tips for July 2010	
July 14	ST05-011 Effectively Erasing Files
July 28	ST05-012 Supplementing Passwords

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 July 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.

Microsoft later released the out-of-band Security Bulletin MS10-046 to address the .LNK vulnerability on August 2, 2010.

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 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: 0xCB0CBD6E
PGP Key Fingerprint: 2A10 30D4 3083 2D28 032F 6DE3 3D60 3D81 CB0C BD6E
PGP Key: https://www.us-cert.gov/pgp/info.asc