US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary
- July 2011 -

This report summarizes general activity including updates to the National Cyber Alert System in July 2011. 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 2011, US-CERT issued 12 Current Activity entries, three Technical Cyber Security Alerts, one Cyber Security Alert, four weekly Cyber Security Bulletins, and one Cyber Security Tip.

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

Contents

Current Activity

Current Activity entries are high-impact security threats and vulnerabilities currently 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 2011	
July 5	Internet System Consortium releases BIND Patches
July 7	Microsoft Releases Advance Notification for July Security Bulletin
July 12	Microsoft Releases July Security Bulletin
July 13	Mozilla Releases Firefox 5.0.1
July 14	VideoLAN Releases VLC Media Player Security Advisories
July 15	RIM Releases Security Advisory for BlackBerry Enterprise Server
July 15	Oracle Releases Patch Update Pre-Release Announcement
July 18	Apple Releases iOS 4.3.4 and iOS 4.2.9
July 19	Oracle Releases Critical Patch Update for July 2011
July 21	Apple Releases Safari 5.1 and 5.0.6

Current Activity for July 2011	
July 21	Foxit Releases Foxit Reader 5.0.2
July 26	Apple Releases iOS 4.3.5 and iOS 4.2.10

- The Microsoft Security Bulletin Summary for July 2011 provided updates to address vulnerabilities in Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, and Microsoft Visio 2003. These vulnerabilities may allow an attacker to execute arbitrary code or operate with elevated privileges.

- Apple released four iOS updates and two Safari updates:

  o iOS 4.3.4 for the iPhone (GSM model), iPod touch, and iPad and iOS 4.2.9 for the iPhone (CDMA model) addressed multiple vulnerabilities that may allow an attacker to execute arbitrary code or operate with escalated privileges.

  o iOS 4.3.5 for the iPhone (GSM model), iPod touch, and iPad and iOS 4.2.10 for the iPhone (CDMA model) addressed a vulnerability that may allow an attacker with a privileged network position to capture or modify data in SSL/TLS sessions.

  o Safari 5.1 and 5.0.6 addressed multiple vulnerabilities that may allow an attacker to execute arbitrary code, perform a cross-site scripting attack, or disclose sensitive information.

- Mozilla released Firefox 5.0.1 to address an issue with Mac OS X 10.7 and Java for Mac OS X 10.6 Update 5, which could cause Firefox to crash.

- Oracle released its Critical Patch Update for July 2011 to address 78 vulnerabilities across multiple products, including Oracle Database Server, Oracle Secure Backup, Oracle Fusion Middleware, Oracle Enterprise Manager, Oracle E-Business Suite, Oracle Supply Chain Products Suite, Oracle PeopleSoft and JDEdwards Suite, and Oracle Sun Products Suite.

Technical Cyber Security Alerts

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

Technical Cyber Security Alerts for July 2011	
July 12	TA11-193A Microsoft Updates for Multiple Vulnerabilities
July 19	TA11-200A Security Recommendations to Prevent Cyber Intrusions
July 20	TA11-201A Oracle Updates for Multiple Vulnerabilities

Cyber Security Alerts

Cyber Security Alerts 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 2011	
July 12	SA11-193A 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.

Cyber Security Bulletins for July 2011	
July 6	SB11-185 Vulnerability Summary for the Week of June 27, 2011
July 11	SB11-192 Vulnerability Summary for the Week of July 4, 2011
July 18	SB11-199 Vulnerability Summary for the Week of July 11, 2011
July 25	SB11-206 Vulnerability Summary for the Week of July 18, 2011

A total of 268 vulnerabilities were recorded in the NVD during July 2011.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users. The focus of July's tip was Internet Service Providers (ISPs).

Cyber Security Tips for July 2011	
July 6	ST04-024 Understanding ISPs

Security Highlights

Apple Releases Multiple Updates

Apple released four iOS updates and two Safari updates during July 2011. iOS 4.3.4 for the iPhone (GSM model), iPod touch, and iPad and iOS 4.2.9 for the iPhone (CDMA model) addressed multiple vulnerabilities that may allow an attacker to execute arbitrary code or operate with escalated privileges. iOS 4.3.5 for the iPhone (GSM model), iPod touch, and iPad and iOS 4.2.10 for the iPhone (CDMA model) addressed a vulnerability that may allow an attacker with a privileged network position to capture or modify data in SSL/TLS sessions. Safari 5.1 and 5.0.6 addressed multiple vulnerabilities that may allow an attacker to execute arbitrary code, perform a cross-site scripting attack, or disclose sensitive information.

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