US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary

- July 2012 -

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

Executive Summary

During July 2012, US-CERT issued eight Current Activity entries, one Alert, and five weekly Bulletins.

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

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 2012	
July 5	Microsoft Releases Advance Notification for July Security Bulletin
July 10	Microsoft Releases July Security Bulletin
July 12	Cisco Releases Multiple Security Advisories for TelePresence
July 12	Microsoft Releases a Security Advisory for Microsoft Digital Certificates
July 12	Microsoft Releases a Security Advisory for Windows Sidebar and Gadgets
July 13	Google Releases Google Chrome 20.0.1132.57
July 18	Oracle Releases Critical Patch Update for July 2012
July 18	Mozilla Releases Multiple Updates

- Microsoft released its monthly Security Bulletin and several Security Advisories:
  - Microsoft released updates to address vulnerabilities in Microsoft Windows, Internet Explorer, Office, Developer Tools, and Server Software as part of the Microsoft Security Bulletin summary for July 2012. These vulnerabilities may allow an attacker to execute arbitrary code, operate with elevated privileges, or disclose sensitive information.

- Microsoft issued Security Advisory 2728973 to replace a number of certificates that did not meet Microsoft's high standard of Public-Key Infrastructure (PKI) management. This update places the intermediate certificate authority (CA) certificates in the Untrusted Certificate Store and replaces them with new certificates that meet Microsoft's PKI standards.
- Security Advisory 2719662 addressed a vulnerability in Microsoft Windows Sidebar and Gadgets. This vulnerability may allow an attacker to execute arbitrary code, take control of an affected system, or disclose sensitive information. This advisory indicates that the workaround does not correct the vulnerability, but it may help mitigate the risk against known attack vectors by disabling the Windows Sidebar and Gadgets.

- Google released Google Chrome 20.0.1132.57 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.
- Cisco released security advisories to address multiple vulnerabilities affecting Cisco's Telepresence Manager, Recoding Server, Multipoint Switch, and Immersive Endpoint System. These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, or inject commands.
- Oracle released its Critical Patch Update for July 2012 to address 87 vulnerabilities across multiple products. This update contains security fixes for Oracle Database Server, Application Express Listener, Secure Backup, Fusion Middleware, Hyperion, Enterprise Manager Grid Control, E-Business Suite, Supply Chain products, PeopleSoft products, Siebel CRM, Industry Applications, Sun products, and MySQL. Additional information regarding Outside In vulnerabilities can be found in the US-CERT Vulnerability Note VU#118913.
- The Mozilla Foundation released updates to address multiple vulnerabilities in Firefox 14, Firefox ESR 10.0.6, Thunderbird 14, Thunderbird ESR 10.0.6, and SeaMonkey 2.11. These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, disclose sensitive information, operate with elevated privileges, bypass security restrictions, or perform a cross-site scripting attack. US-CERT encourages users and administrators to review the Mozilla Foundation Advisory for Firefox 14, Firefox ESR 10.0.6, Thunderbird 14, Thunderbird ESR 10.0.6, and SeaMonkey 2.11 and apply any necessary updates to help mitigate the risk.

Alerts

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

Alerts for July 2012	
July 10	TA12-192A Microsoft Updates for Multiple Vulnerabilities

Bulletins

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.

Bulletins for July 2012	
July 2	SB12-184 Vulnerability Summary for the Week of June 25, 2012
July 9	SB12-191 Vulnerability Summary for the Week of July 2, 2012
July 16	SB12-198 Vulnerability Summary for the Week of July 9, 2012
July 23	SB12-205 Vulnerability Summary for the Week of July 16, 2012
July 30	SB12-212 Vulnerability Summary for the Week of July 23, 2012

A total of 536 vulnerabilities were recorded in the NVD during July 2012.

Security Highlights

Microsoft Releases a Security Advisory for Microsoft Digital Certificates

Microsoft has released security advisory 2728973 to replace a number of certificates that did not meet Microsoft's high standard of Public-Key Infrastructure (PKI) management. This update places the intermediate certificate authority (CA) certificates in the Untrusted Certificate Store and replaces them with new certificates that meet Microsoft's PKI standards.

US-CERT encourages users and administrators to review Microsoft Security Advisory 2728973 and take any necessary action to help mitigate this 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: soc@us-cert.gov
Phone Number: +1 888-282-0870
PGP/GPG Key: 0x91D70D64
PGP Key Fingerprint: F68D 07E5 FC48 403F C989 AC73 2A4C 5804 0FA6 ED7D
PGP Key: https://www.us-cert.gov/pgp/soc.asc