US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary

- April 2012 -

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

Executive Summary

During April 2012, US-CERT issued 12 Current Activity entries, two Alerts, and five weekly Bulletins.

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

Contents

Current Activity

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

Current Activity for April 2012	
April 4	Apple Update for Java for OS X Lion and Mac OS X
April 5	Cisco Releases Security Advisory for WebEx Player
April 5	Google Releases Google Chrome 18.0.1025.151
April 5	Microsoft Releases Advance Notification for April Security Bulletin
April 10	Microsoft Releases April Security Bulletin
April 10	Adobe Releases Security Bulletin for Adobe Reader and Acrobat
April 11	Samba Releases Updates for 3.0.x – 3.6.3
April 12	HP ProCurve 5400 zl Switches Security Bulletin
April 16	Apple Releases Flashback Malware Security Updates
April 18	Oracle Releases Critical Patch Update for April 2012
April 24	DNSChanger Malware
April 24	RuggedCom Rugged Operating System Vulnerability

- Microsoft released updates to address vulnerabilities in Microsoft Windows, Internet Explorer, .NET Framework, Office, SQL Server, Server Software, Developer Tools, and Forefront United Access Gateway as part of the Microsoft Security Bulletin Summary for April 2012. These vulnerabilities may allow an attacker to execute arbitrary code or disclose sensitive information.
- Adobe released security bulletin APSB12-08 to address multiple vulnerabilities in Adobe Reader X (10.1.2) and earlier versions for Windows and Macintosh, Adobe Reader 9.4.6 and earlier versions for Linux, and Adobe Acrobat X (10.1.2) and earlier versions for Windows and Macintosh. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition.
- Apple has released Java and security updates to address the Flashback malware in OS X Lion v10.7.3, OS X Lion Server v10.7.3, Mac OS X v10.6.8, Mac OS X Server v10.6.8. Apple also released a malware removal tool for the most common variant of the Flashback malware. If the malware is discovered, the tool will notify the user and remove it automatically. If the malware is not discovered, no indication will be given.
- Cisco released security advisory cisco-sa-20120404-webex to address multiple vulnerabilities in the Cisco WebEx Player. These vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition.
- Google released Chrome 18.0.1025.151 for Linux, Macintosh, 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. US-CERT encourages users and administrators to review the Google Chrome Release blog entry and update to Chrome 18.0.1025.151.
- Samba released an update to address a vulnerability in Samba version 3.6.3 and all previous versions. Exploitation of this vulnerability may allow a remote attacker to use anonymous connections to execute arbitrary code with root privileges. US-CERT encourages users and administrators to review the recent Samba Security Announcement and apply any necessary updates to help mitigate the risk.
- Hewlett-Packard (HP) released a security bulletin to address a security vulnerability affecting HP 5400 zl series switches purchased after April 30, 2011. These switches contain a compact flash card that may be infected with malware. US-CERT encourages users and administrators to review HP Security Bulletin HPSBPV02754, which includes a list of infected switches and serial numbers, and apply any necessary steps to help mitigate the risk.
- Oracle has released its Critical Patch Update for April 2012 to address 88 vulnerabilities across multiple products. US-CERT encourages users and administrators to review the April 2012 Critical Patch Update and apply any necessary updates to help mitigate the risks.

Alerts

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

Alerts for April 2012	
April 10	TA12-101A Microsoft Updates for Multiple Vulnerabilities
April 10	TA12-101B Adobe Reader and Acrobat Security Updates and Architectural Improvements

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 April 2012	
April 2	SB12-093 Vulnerability Summary for the Week of March 26, 2012
April 9	SB12-100 Vulnerability Summary for the Week of April 2, 2012
April 16	SB12-107 Vulnerability Summary for the Week of April 9, 2012
April 23	SB12-114 Vulnerability Summary for the Week of April 16, 2012
April 30	SB12-121 Vulnerability Summary for the Week of April 23, 2012

A total of 228 vulnerabilities were recorded in the NVD during April 2012.

Security Highlights

DNSChanger Malware

US-CERT encourages users and administrators to ensure their systems are not infected with the DNSChanger malware by utilizing tools and resources available at the DNS Changer Working Group (DCWG) website. Computers testing positive for infection of DNSChanger malware will need to be cleaned of the malware in order to maintain continued internet connectivity beyond July 9, 2012.

On November 8, 2011, the FBI, NASA-OIG (Office of Inspector General), and Estonian police arrested several cyber criminals in "Operation Ghost Click." The criminals operated under the company name "Rove Digital," and distributed DNS changing viruses, variously known as TDSS, Alureon, TidServ, and TDL4 viruses.

Additional information about Operation Ghost Click and the DNSChanger malware is available at the FBI website.

RuggedCom Rugged Operating System Vulnerability

RuggedCom Rugged Operating System (ROS), used in RuggedCom network infrastructure devices, contains a hard-coded user account with a predictable password. This user account cannot be manually disabled. An attacker who successfully guesses the password may be able to gain complete administrative control of the ROS device.

As a workaround, RuggedCom has recommended disabling the rsh service and setting the number of telnet connections allowed to 0. For more information, please see US-CERT Vulnerability Note VU#889195.

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 send email to 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