US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary

- March 2012 -

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

Executive Summary

During March 2012, US-CERT issued 13 Current Activity entries, one Alert, and four weekly Bulletins.

Highlights for this month include updates or advisories released by Microsoft, Adobe, Cisco, Google, 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 March 2012	
March 5	Google Releases Chrome 17.0.963.65
March 5	Adobe Releases Update for Adobe Flash Player
March 7	DNSChanger Malware
March 9	Apple Releases Multiple Security Updates
March 12	Google Releases Chrome 17.0.963.79
March 13	Apple Releases Safari 5.1.4
March 13	Microsoft Releases March Security Bulletin
March 14	Mozilla Releases Multiple Updates
March 14	Cisco Releases Multiple Security Advisories
March 22	Google Releases Google Chrome 17.0.963.83
March 28	Adobe Releases Security Advisory for Adobe Flash Player
March 28	Cisco Releases Multiple Security Advisories
March 29	Google Releases Google Chrome 18.0.1025.142

- Microsoft released updates to address vulnerabilities in Microsoft Windows, Visual Studio, and Express Design as part of the Microsoft Security Bulletin Summary for March 2012. These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, or operate with elevated privileges.
- Adobe released two Security Advisories to address vulnerabilities affecting Adobe Flash Player. Exploitation of these vulnerabilities may allow an attacker to take control of the affected system or cause a denial-of-service condition. Affected software versions include the following:
    - Adobe Flash Player 11.1.102.63 and earlier versions from Windows, Linux, and Solaris operating systems
    - Adobe Flash Player 11.1.115.6 and earlier versions for Android 4.x
    - Adobe Flash Player 11.1.111.7 and earlier versions for Android 3.x and 2.x
    - Adobe Air 3.1.0.4880 and earlier versions for Windows, Macintosh, and Android
- Cisco released security advisories to address vulnerabilities affecting the following products:
    - Cisco ASA 5500 Series Adaptive Security Appliances (ASA)
    - Cisco Catalyst 6500 Series ASA Service Module (ASASM)
    - Cisco Catalyst 6500 Series Firewall Service Module (FWSM)
    - Cisco Adaptive Security Appliance Software 7.1 and 7.2
    - Cisco Adaptive Security Appliance Software 8.0, 8.1, 8.2, 8.3, 8.4, 8.6
    - Cisco IOS Software

  US-CERT encourages users and administrators to review Cisco Security Advisories cisco-sa-20120314-asa, cisco-sa-20120314-fwsm, cisco-sa-20120314-asaclient, cisco-sa-20120328-ssh, cisco-sa-20120328-rsvp, cisco-sa-20120328-mace, cisco-sa-20120328-msdp, cisco-sa-20120328-nat, cisco-sa-20120328-ike, cisco-sa-20120328-smartinstall, cisco-sa-20120328-pai, and cisco-sa-20120328-zbfw and apply any necessary updates to help mitigate the risks.
- Google released Chrome versions 17.0.963.65, 17.0.963.79, 17.0.963.83, and 18.0.1025.142 for Linux, Mac, Windows, and Chrome Frame to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, or perform a cross-site scripting attack.
- The Mozilla Foundation released updates for Firefox 11, Firefox 3.6.28, Firefox ESR 10.0.3, Thunderbird 11, Thunderbird 3.1.20, Thunderbird ESR 10.0.3, and SeaMonkey 2.8 to address vulnerabilities that may allow an attacker to execute arbitrary code, cause a denial-of-service condition, bypass security restrictions, operate with escalated privileges, or perform a cross-site scripting attack.

Alerts

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

Alerts for March 2012	
March 13	TA12-073A Microsoft Updates for Multiple Vulnerabilities

Bulletins

Bulletins are issued weekly and provide a summary of new vulnerabilities recorded in 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 March 2012	
March 5	SB12-065 Vulnerability Summary for the Week of February 27, 2012
March 12	SB12-072 Vulnerability Summary for the Week of March 5, 2012
March 19	SB12-079 Vulnerability Summary for the Week of March 12, 2012
March 26	SB12-086 Vulnerability Summary for the Week of March 19, 2012

A total of 393 vulnerabilities were recorded in the NVD during March 2012.

Security Highlights

DNSChanger Malware

UPDATE: On March 5, 2012, a federal judge agreed to allow more time for organizations and individuals to clean systems of the DNSChanger malware and extended the deadline for shutting off servers that had been keeping infected computers connected to the Internet.

Although the new deadline is July 9, 2012, US-CERT strongly recommends that organizations and individuals who have not verified that their systems are free of the DNSChanger malware do so as soon as possible. Please refer to the previous entry (see below) for background information and resources on detection and removal of the malware.

In November 2011, U.S. Federal prosecutors announced Operation Ghost Click, an investigation that resulted in the arrests of a ring of seven people who allegedly infected millions of computers with DNSChanger malware.

The malware may prevent users' anti-virus software from functioning properly and hijack the domain name system (DNS) on infected systems. Systems affected by DNS hijacking may send Internet requests to a rogue DNS server rather than a legitimate one.

To prevent millions of Internet users infected with the DNSChanger malware from losing Internet connectivity when the members of the ring where arrested, the FBI replaced rogue DNS servers with clean servers.

However, the court order allowing the FBI to provide the clean servers is set to expire on March 8, 2012. Computers that are infected with the DNSChanger malware may lose Internet connectivity when these FBI servers are taken offline.

US-CERT encourages users and administrators to utilize the FBI's rogue DNS detection tool to ensure their systems are not infected with the DNSChanger malware. Computers testing positive for infection of the DNSChanger malware will need to be cleaned of the malware to ensure continued Internet connectivity.

Users and administrators are encouraged to implement the following preventative measures to protect themselves from malware campaigns:

- Maintain up-to-date antivirus software.
- Do not follow unsolicited web links in email messages.
- Configure your web browser as described in the Securing Your Web Browser document.
- Use caution when opening email attachments. Refer to the Using Caution with Email Attachments Cyber Security Tip for more information on safely handling email attachments.
- Implement best security practices as described in the Ten Ways to Improve the Security of a New Computer (pdf) document.

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: info@us-cert.gov
Phone Number: +1 (703) 235-5110
PGP Key ID: 0xEDA10949
PGP Key Fingerprint: 5A24 6040 50FC 1BA3 81FA 0919 1378 C036 EDA1 0949
PGP Key: https://www.us-cert.gov/pgp/info.asc