US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary
- November 2012 -

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

Executive Summary

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

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

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 November 2012	
November 1	Cisco Releases Security Advisory for Cisco Prime Data Center Network Manager
November 6	Security Updates Available for Adobe Flash Player
November 7	Google Releases Google Chrome 23.0.1271.64
November 8	Cisco Releases Security Advisory for Cisco Secure Access Control System (ACS)
November 13	Microsoft Releases November 2012 Security Bulletin
November 20	Holiday Season Phishing Scams and Malware Campaigns
November 20	Adobe Releases Security Update for ColdFusion
November 21	Mozilla Releases Multiple Updates
November 27	Google Releases Google Chrome 23.0.1271.91

- Cisco released the following security advisories:
    - A security advisory for Cisco Prime Data Center Network Manager (DCNM) addressed a vulnerability that may allow a remote, unauthenticated attacker to execute arbitrary commands on the computer that is running the Cisco Prime DCNM application. Cisco

released software updates that address this vulnerability. US-CERT encourages users and administrators of this software to review Cisco Security Advisory 20121031-DCNM and follow best-practice security guidelines to determine if their organization is affected and the appropriate response.

  - A security advisory for Cisco Secure Access Control Systems (ACS) addressed a vulnerability that could allow an unauthenticated, remote attacker to bypass the TACACS+ based authentication service offered by the product. Cisco released software updates that address this vulnerability. US-CERT encourages users and administrators to review the Cisco Security Advisory 20121107-ACS and follow best-practice security policies to determine if their organization is affected and the appropriate response.

- Adobe released the following security updates:
  - Security Updates for Adobe Flash Player addressed vulnerabilities that could cause a crash and potentially allow an attacker to take control of the affected system. Secure updates are available for the following versions of Adobe Flash Player: Adobe Flash Player 11.4.402.287 and earlier versions for Windows and Macintosh, Adobe Flash Player 11.2.202.243 and earlier versions for Linux, Adobe Flash Player 11.1.115.20 and earlier versions for Android 4.x, and Adobe Flash Player 11.1.111.19 and earlier versions for Android 3.x and 2.x. US-CERT encourages users and administrators to review Adobe Security Bulletin APSB12-24 and follow best-practice security policies to determine if their organization is affected and the appropriate response.
  - A security hotfix for ColdFusion 10 Update 1 and above for Windows resolved a vulnerability affecting ColdFusion on Windows Internet Information Services (IIS) that could result in a denial of service. US-CERT encourages users and administrators to review Adobe Security Bulletin APSB12-25 to determine which updates should be applied.
- Google released Google Chrome 23.0.1271.64 for Windows, Macintosh, Linux, and Chrome Frame to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code. Google also released Google Chrome 23.0.1271.91 for Windows, Mac, Linux, and ChromeFrame to address multiple vulnerabilities. These vulnerabilities could result in a denial of service or allow an attacker to execute arbitrary code. US-CERT encourages users and administrators to review the Google Chrome Release blog entry and update to Chrome 23.0.1271.91.
- Microsoft released updates to address vulnerabilities in Microsoft Windows Shell, .NET Framework, Windows Kernel-mode drivers, Excel, Internet Information Services (IIS), and cumulative security updates for Internet Explorer as part of the Microsoft Security Bulletin Summary for November 2012. These vulnerabilities may allow an attacker to execute arbitrary code remotely, operate with elevated privileges, or cause a denial-of-service condition. US-CERT encourages users and administrators to review the bulletin and follow best-practice security policies to determine which updates should be applied.

Alerts

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

Alerts for November 2012	
November 13	TA12-318A 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 November 2012	
November 5	SB12-310 Vulnerability Summary for the Week of October 29, 2012
November 12	SB12-317 Vulnerability Summary for the Week of November 5, 2012
November 19	SB12-324 Vulnerability Summary for the Week of November 12, 2012
November 26	SB12-331 Vulnerability Summary for the Week of November 19, 2012

A total of 417 vulnerabilities were recorded in the NVD during November 2012.

Security Highlights

Holiday Season Phishing Scams and Malware Campaigns

Since the winter holidays are quickly approaching, US-CERT is republishing this entry to increase awareness about phishing scams and malware campaigns.

In the past, US-CERT has received reports of an increased number of phishing scams and malware campaigns that take advantage of the winter holidays and holiday shopping season. Users who are new to making seasonal online purchases are encouraged to take care and use safe online shopping habits. US-CERT reminds users to remain cautious when receiving unsolicited email messages that could be part of a potential phishing scam or malware campaign.

These phishing scams and malware campaigns may include but are not limited to the following:

- electronic greeting cards that may contain malware
- requests for charitable contributions that may be phishing scams and may originate from illegitimate sources claiming to be charities
- screensavers or other forms of media that may contain malware
- credit card applications that may be phishing scams or identity theft attempts
- online shopping advertisements that may be phishing scams or identity theft attempts from bogus retailers

US-CERT encourages users and administrators to use caution when encountering these types of email messages and take the following preventative measures to protect themselves from phishing scams and malware campaigns:

- Refer to the Shopping Safely Online Cyber Security Tip for more information on online shopping safety.

- Do not follow unsolicited web links in email messages.
- 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.
- Maintain up-to-date antivirus software.
- Review the Federal Trade Commission's Charity Checklist.
- Verify charity authenticity through a trusted contact number. Trusted contact information can be found on the Better Business Bureau's National Charity Report Index.
- Refer to the Recognizing and Avoiding Email Scams (pdf) document for more information on avoiding email scams.
- Refer to the Avoiding Social Engineering and Phishing Attacks Cyber Security Tip for more information on social engineering attacks.

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.

Website Address: http://www.us-cert.gov
Email Address: soc@us-cert.gov
Phone Number: +1 888-282-0870
PGP/GPG Key: 0xE96C965B
PGP Key Fingerprint: 3EC2 7B68 B072 B65C 9044 BE9C 07B7 E916 BDE5 AC10
PGP Key: http://www.us-cert.gov/pgp/info.asc