US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary

- January 2012 -

This report summarizes general activity including updates to the National Cyber Alert System in January 2012. It includes current activity updates, technical and non-technical cyber security alerts, and cyber security bulletins, in addition to other newsworthy events or highlights.

Executive Summary

During January 2012, US-CERT issued 10 Current Activity entries, three Technical Cyber Security Alerts, two Cyber Security Alerts, and five weekly Cyber Security Bulletins.

Highlights for this month include updates or advisories released by Microsoft, Adobe, Oracle, Google, and Symantec, as well as a phishing and malware campaign using spoofed US-CERT email addresses.

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; following that is a brief overview of the most significant entries.

Current Activity for January 2012	
January 5	Microsoft Releases Advance Notification for January Security Bulletin
January 6	Google Releases Chrome 16.0.912.75
January 10	Adobe Releases Security Advisory for Adobe Reader and Acrobat
January 11	Microsoft Releases January Security Bulletin
January 12	Phishing Campaign Using Spoofed US-CERT Email Addresses
January 18	Oracle Releases Critical Patch Update for January 2012
January 19	Best Practices for Recovery from the Malicious Erasure of Files
January 24	Symantec pcAnywhere Hotfix
January 24	Google Releases Chrome 16.0.912.77
January 24	Denial-of-Service Malware Campaign

- Microsoft released updates to address vulnerabilities in Microsoft Windows and Microsoft Developer Tools and Software as part of the Microsoft Security Bulletin Summary for January 2012. These vulnerabilities may allow an attacker to execute arbitrary code, operate with elevated privileges, obtain sensitive information, and bypass security restrictions.
- Adobe released Security Advisory APSB12-01 to address a vulnerability affecting Adobe Reader and Adobe Acrobat. Exploitation of these vulnerabilities may allow an attacker to cause a denial-of-service condition or take control of the affected system. Affected software versions include
  - Adobe Reader X (10.1.1) and earlier 10.x versions for Windows and Macintosh,
  - Adobe Reader 9.4.7 and earlier 9.x versions for Windows,
  - Adobe Reader 9.4.6 and earlier 9.x versions for Macintosh,
  - Adobe Acrobat X (10.1.1) and earlier 10.x versions for Windows and Macintosh,
  - Adobe Acrobat 9.4.7 and earlier 9.x versions for Windows, and
  - Acrobat 9.4.6 and earlier 9.x versions for Macintosh.
- Oracle released its Critical Patch Update for January 2012 to address 78 vulnerabilities across multiple products. Security fixes include
  - 2 for Oracle Database Server,
  - 1 for Oracle Fusion Middleware,
  - 3 for Oracle E-Business Suite,
  - 1 for Oracle Supply Chain Products Suite,
  - 6 for Oracle PeopleSoft Products,
  - 8 for Oracle JD Edwards Products,
  - 17 for Oracle Sun Products Suite,
  - 3 for Oracle Virtualization, and
  - 27 for Oracle MySQL.
- Google released Chrome 16.0.912.75 and Chrome 16.0.912.77 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.
- Symantec released an update for pcAnywhere to address multiple vulnerabilities for the following software versions running on Windows:
  - pcAnywhere 12.5 SP3 and
  - pcAnywhere Solutions 7.1 GA, SP 1, and SP 2

Technical Cyber Security Alerts

Technical Cyber Security Alerts provide timely information about current security issues, vulnerabilities, and exploits. The following table lists the Technical Cyber Security Alerts that were posted this month.

Technical Cyber Security Alerts for January 2012	
January 6	TA12-006A Wi-Fi Protected Setup (WPS) Vulnerable to Brute-Force Attack
January 10	TA12-010A Microsoft Updates for Multiple Vulnerabilities
January 24	TA12-024A “Anonymous” DDoS Activity

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. The following table lists the Cyber Security Alerts that were posted this month.

Cyber Security Alerts (non-technical) for January 2012	
January 6	SA12-006A Wi-Fi Protected Setup (WPS) Vulnerable to Brute-Force Attack
January 10	SA12-010A 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 (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. The following table lists the Cyber Security Bulletins that were posted this month.

Cyber Security Bulletins for January 2012	
January 3	SB12-002 Vulnerability Summary for the Week of December 26, 2011
January 9	SB12-009 Vulnerability Summary for the Week of January 2, 2012
January 17	SB12-016 Vulnerability Summary for the Week of January 9, 2012
January 23	SB12-023 Vulnerability Summary for the Week of January 16, 2012
January 30	SB12-030 Vulnerability Summary for the Week of January 23, 2012

A total of 396 vulnerabilities were recorded in the NVD during January 2012.

Security Highlights

Phishing Campaign Using Spoofed US-CERT Email Addresses

On January 10, 2012, US-CERT received reports of a phishing campaign that is spoofing US-CERT email to deliver a variant of the Zeus/Zbot Trojan known as Ice-IX. This campaign appears to be targeting a large number of private sector organizations as well as federal, state, and local governments.

US-CERT advises that users do not open the email or any of the attachments and promptly delete the email from their inboxes.

Reports indicate that SOC@US-CERT.GOV is the primary email address being spoofed, but other invalid email addresses are also being used.

The subject of the phishing email is: “Phishing incident report call number: PH000000XXXXXXX” with the “X” containing an incident report number that varies.

The attached zip file is titled “US-CERT Operation Center Report XXXXXXX.zip” with “X” indicating a random value or string. The zip attachment contains an executable file with the name “US-CERT Operation CENTER Reports.eml.exe”, which is a variant of the Zeus/Zbot Trojan known as Ice-IX.

US-CERT encourages users to do the following to reduce the risks associated with this and other phishing campaigns:

- Do not open the attachments in email messages from unknown sources.
- Install anti-virus software and keep virus signatures files up to date.
- 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 page for information on social engineering attacks.
- Refer to the Recovering from Viruses, Worms, and Trojan Horses page for additional information on how to recover from malware.

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 send email to info@us-cert.gov.

Web Site Address: http://www.us-cert.gov
Email Address: info@us-cert.gov
Phone Number: +1 (888) 282-0870
PGP Key ID: 0xEDA10949
PGP Key Fingerprint: 6040 50FC 1BA3 81FA 0919 1378 C036 EDA1 0949
PGP Key: https://www.us-cert.gov/pgp/info.asc