US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary
- February 2010 -

This report summarizes general activity as well as updates made to the National Cyber Alert System for February 2010. It includes current activity updates, technical and non-technical cyber security alerts, cyber security bulletins, and cyber security tips, in addition to other newsworthy events or highlights.

Executive Summary

During February 2010, US-CERT issued 11 Current Activity entries, two (2) Technical Cyber Security Alerts, one (1) Cyber Security Alert, five (5) weekly Cyber Security Bulletins, and two (2) Cyber Security Tips.

Highlights for this month include updates released by Adobe, Apple, Cisco, Google, Microsoft, Mozilla, and Oracle and malicious activity related to the "Aurora" Internet Explorer (IE) exploit.

Contents

Current Activity

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

Current Activity for February 2010	
February 3	Microsoft Releases Security Advisory 980088
February 4	Apple Releases iPhone OS 3.1.3 and iPhone OS 3.1.3 for iPod Touch
February 4	Microsoft Releases Advance Notification for February Security Bulletin
February 7	Oracle Releases Security Alert for WebLogic Server Vulnerability
February 9	Microsoft Releases February Security Bulletin
February 10	Cisco Releases Advisory for IronPort Encryption Appliance
February 12	Google Releases Chrome 4.0.249.89
February 12	Adobe Releases Security Bulletins for Acrobat, Reader, and Flash Player

Current Activity for February 2010	
February 17	Cisco Releases Multiple Security Advisories
February 18	Mozilla Releases Security Advisories
February 24	Adobe Releases a Security Update for Download Manager

- Microsoft released updates for IE, Windows, and Office.
  - Microsoft released Security Advisory 980088 to alert users to a vulnerability in Microsoft IE. This vulnerability may allow an attacker to harvest user credentials and other sensitive information by enticing users to visit a maliciously crafted web page. Review the security advisory and apply the suggested workarounds to help mitigate risks.
  - Microsoft released an update to address vulnerabilities in Microsoft Windows and Office as part of the Microsoft Security Bulletin Summary for February 2010. These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, or operate with elevated privileges. Review the bulletin for additional information.
- Apple released iPhone OS 3.1.3 and iPhone OS 3.1.3 for iPod touch to address vulnerabilities in the CoreAudio, ImageIO, Recovery Mode, and WebKit packages. These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, or obtain sensitive information.
- Oracle released a security alert to address a vulnerability in Oracle WebLogic Server. This vulnerability may allow a remote, unauthenticated attacker to execute arbitrary commands on an affected system. Review the security alert and apply any necessary updates to mitigate the risk.
- Google released Chrome 4.0.249.89 for Windows to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code or obtain sensitive information. Review the Google Chrome Releases blog entry and update to Chrome 4.0.249.89 for Windows to help mitigate the risks.
- Adobe released three security bulletins to address vulnerabilities in Adobe Acrobat, Reader, Flash Player, and Download Manager.
  - Security Bulletin APSB10-06 updates Adobe Flash Player and Adobe AIR to address a critical vulnerability. This vulnerability may allow an attacker to make unauthorized cross-domain requests or create a potential denial-of-service issue.
  - Security Bulletin APSB10-07 addressed two critical vulnerabilities are available for Adobe Reader and Acrobat. These vulnerabilities may allow an attacker to execute arbitrary code, make unauthorized cross-domain requests, or cause a denial-of-service condition.
  - Security Bulletin APSB10-08 addressed a vulnerability in the Adobe Download Manager that could allow an attacker to download and install unauthorized software.
- Cisco released four security advisories to address vulnerabilities in multiple products.
  - Security Advisory cisco-sa-20100210-ironport addressed multiple vulnerabilities in IronPort Encryption Appliance. These vulnerabilities may allow a remote, unauthenticated attacker to execute arbitrary code or obtain sensitive information. Additional information regarding these vulnerabilities can be found in Cisco Applied Mitigation Bulletin 111668.
  - Security advisory cisco-sa-20100217-fwsm addresses a vulnerability in the Cisco Firewall Services Module (FWSM) for the Cisco Catalyst 6500 Series Switches and Cisco 7600

Series Routers. Successful and repeated exploitation of this vulnerability could result in a denial-of-service condition.

- Security advisory cisco-sa-20100217-asa addresses multiple vulnerabilities in Cisco ASA 5500 Series Adaptive Security Appliances. These vulnerabilities may allow an attacker to gain unauthorized access to an affected system or cause a denial-of-service condition.
- Security advisory cisco-sa-20100217-csa addresses multiple vulnerabilities in the Cisco Security Agent. These vulnerabilities may allow an attacker to execute arbitrary SQL commands, view and download arbitrary files, or cause a denial-of-service condition.

Technical Cyber Security Alerts

Technical Cyber Security Alerts are distributed to provide timely information about current security issues, vulnerabilities, and exploits.

Technical Cyber Security Alerts for February 2010	
February 9	TA10-040A Microsoft Updates for Multiple Vulnerabilities
February 24	TA10-055A Malicious Activity Associated with "Aurora" Internet Explorer Exploit

Cyber Security Alerts

Cyber Security Alerts are distributed to 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.

Cyber Security Alerts (non-technical) for February 2010	
February 9	SA10-040A 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.

Security Bulletins for February 2010
SB10-032 Vulnerability Summary for the Week of January 25, 2010
SB10-040 Vulnerability Summary for the Week of February 1, 2010
SB10-046 Vulnerability Summary for the Week of February 8, 2010
SB10-053 Vulnerability Summary for the Week of February 15, 2010

A total of 308 vulnerabilities were recorded in the NVD during February 2010.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users. The February tips focused on operating systems and web browsers. Links to the full versions of these documents are listed below.

Cyber Security Tips for February 2010	
February 11	ST04-021 Understanding Your Computer: Operating Systems
February 25	ST04-022 Understanding Your Computer: Web Browsers

Security Highlights

Malicious Activity Associated with "Aurora" Internet Explorer Exploit

Malicious activity detected in mid-December targeted at least 20 organizations representing multiple industries including chemical, finance, information technology, and media. Investigation into this activity revealed that third parties routinely accessed the personal email accounts of dozens of users based in the United States, China, and Europe. Further analysis revealed these users were victims of previous phishing scams through which threat actors successfully gained access to their email accounts. Security experts discovered that one of the malware samples exploited a vulnerability in Microsoft Internet Explorer (IE). Microsoft released Security Bulletin MS10-002, which addressed this IE vulnerability as well as others, and US-CERT provided technical indicators to the public. Additional details are also provided in Technical Cyber Security Alert TA10-055A.

US-CERT encouraged users to take the following precautions to help mitigate the risks:

- As a best practice, limit end-user permissions on systems by granting minimal administrative rights.
- Enable Data Execution Prevention (DEP) for IE 6 Service Pack 2 or IE 7. IE 8 automatically enables DEP.
- Inspect network traffic history for communication with external systems associated with the attack.
- Examine computers for specific files or file attributes related to the attack.

Contacting US-CERT

If you would like to contact US-CERT to ask a question, submit an incident, or to 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 email 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: 0xCB0CBD6E
PGP Key Fingerprint: 2A10 30D4 3083 2D28 032F 6DE3 3D60 3D81 CB0C BD6E
PGP Key: https://www.us-cert.gov/pgp/info.asc