



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary - February 2011 -

This report summarizes general activity including updates to the [National Cyber Alert System](#) in February 2011. 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 2011, US-CERT issued 18 Current Activity entries, one Technical Cyber Security Alert, one Cyber Security Alert, four weekly Cyber Security Bulletins, and one Cyber Security Tip.

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

Contents

Executive Summary	1
Current Activity	1
Technical Cyber Security Alerts	3
Cyber Security Alerts	3
Cyber Security Bulletins	4
Cyber Security Tips	4
Security Highlights	4
Contacting US-CERT	4

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 February 2011	
February 2	Cisco Releases Security Advisory for Multiple Cisco WebEx Player Vulnerabilities
February 2	VideoLAN Releases Security Advisory for VLC Media Player
February 3	Cisco Releases Security Advisory for Tandberg E, EX, and C Series Endpoints
February 3	Microsoft Releases Advance Notification for February Security Bulletin
February 4	Majordomo Vulnerable to Directory Traversal
February 4	Adobe Prenotification Security Advisory for Adobe Reader and Acrobat
February 7	Google Releases Chrome 9.0.597.84
February 8	WordPress Releases Version 3.0.5
February 8	Microsoft Releases February Security Bulletin
February 8	Adobe Releases Updates for Adobe Reader and Acrobat

Current Activity for February 2011	
February 9	RealNetworks, Inc. Releases Security Updates for RealPlayer
February 9	Adobe Releases Security Update for Flash Player
February 10	Google Releases Chrome 9.0.597.95
February 10	Oracle Releases Security Alert for Java Runtime Environment
February 11	VMware Releases Advisory for Windows 7 Users
February 18	Oracle Releases Critical Patch Update for Java SE and Java for Business
February 23	Internet System Consortium Releases BIND Advisory
February 28	Cisco Releases Multiple Security Advisories

- Adobe addressed multiple vulnerabilities in Adobe Reader, Acrobat, and Flash Player.
 - Adobe Security Bulletin [APSB11-03](#) for Reader, and Acrobat addresses multiple vulnerabilities affecting numerous software versions. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, operate with escalated privileges, or conduct cross-site scripting attacks.
 - Adobe Security Bulletin [APSB11-02](#) for Flash Player addresses multiple vulnerabilities in Flash Player 10.1.102.64 and earlier versions for Windows, Macintosh, Linux, and Solaris. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition.
- Microsoft released updates to address vulnerabilities in Microsoft Windows, Internet Explorer, and Office as part of the [Microsoft Security Bulletin Summary for February 2011](#). These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, obtain sensitive information or operate with elevated privileges.
- Google released [Chrome 9.0.597.84](#) and [Chrome 9.0.597.95](#) to address multiple vulnerabilities. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition. Chrome 9.0.597.95 also included a recently released version of Adobe Flash Player that repairs several vulnerabilities.
- Cisco released multiple security advisories to address vulnerabilities in multiple Cisco products. Successful exploitation of these vulnerabilities may allow an attacker to execute arbitrary code, take control of the affected system or device, or cause a denial-of-service condition.
- Oracle released a security alert and a critical patch update advisory for Java SE and Java for Business.
 - [Oracle Security Alert for CVE-2010-4476](#) addresses a vulnerability in the Java Runtime Environment component of the Oracle Java SE and Java for Business products. Exploitation of this vulnerability may allow an attacker to cause a denial-of-service condition.
 - The [Oracle Java SE and Java for Business Critical Patch Update Advisory for February 2011](#) addresses multiple vulnerabilities and contains 21 security fixes for Java SE and Java for Business. US-CERT encourages users and administrators to review and apply any necessary updates to mitigate the risks.

- Mozilla released a fix for a vulnerability affecting Majordomo 2. Exploitation of this vulnerability may allow an attacker to obtain sensitive information that could be used to leverage additional attacks. Reports indicate this vulnerability affects builds 20110121 and prior. US-CERT encourages users and administrators to upgrade to Majordomo 2 build 20110125 and later. The [Sitewatch Advisory](#) provides additional information regarding this vulnerability.
- The Internet System Consortium [advisory](#) addresses a vulnerability affecting BIND versions 9.7.1 through 9.7.2-P3. This vulnerability may allow an attacker to cause a denial-of-service condition. US-CERT Vulnerability Note [VU#559980](#) provides additional information.
- WordPress released [WordPress 3.0.5](#) to address multiple vulnerabilities. Execution of these vulnerabilities may allow an attacker to conduct cross-site scripting attacks or obtain sensitive information.
- The RealNetworks, Inc. [update for RealPlayer](#) addresses multiple vulnerabilities. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code.
- The VMware Security Advisory alerts users to an issue affecting VMware on the Microsoft Windows 7 platform. This issue prevents VMware from connecting from the View Client on Windows 7 to the View Connection Server after installing the Microsoft patches [2482017](#) and [2467023](#) from Microsoft Security Bulletin MS11-003. VMware users on the Windows 7 platform should upgrade to VMware View Client build 353760 prior to applying the Microsoft patches. VMware users who have previously applied these Microsoft patches should upgrade to VMware View Client build 353760 to mitigate the issue.
- [VideoLAN Security Advisory 1102](#) addresses a VLC Media Player vulnerability. This vulnerability may allow an attacker to execute arbitrary code. US-CERT encourages users and administrators to review the Security Advisory and apply any necessary updates or workarounds to help mitigate the risks.

Technical Cyber Security Alerts

[Technical Cyber Security Alerts](#) are distributed to provide timely information about current security issues, vulnerabilities, and exploits.

<i>Technical Cyber Security Alerts for February 2011</i>	
February 8	TA11-039A Microsoft Updates for Multiple Vulnerabilities

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.

<i>Cyber Security Alerts (non-technical) for February 2011</i>	
February 8	SA11-039A 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's (NIST's) [National Vulnerability Database \(NVD\)](#). The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSA)/US-CERT. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

Security Bulletins for February 2011	
	SB11-038 Vulnerability Summary for the Week of January 31, 2011
	SB11-045 Vulnerability Summary for the Week of February 7, 2011
	SB11-052 Vulnerability Summary for the Week of February 14, 2011
	SB11-059 Vulnerability Summary for the Week of February 21, 2011

A total of 378 vulnerabilities were recorded in the NVD during February 2011.

Cyber Security Tips

[Cyber Security Tips](#) are primarily intended for non-technical computer users. The focus of February's tip was common computer use and security myths.

Cyber Security Tips for February 2011	
February 16	ST06-002 Debunking Some Common Myths

Security Highlights

Adobe Releases Security Update for Flash Player

Adobe released a [critical](#) security update for Adobe Flash Player 10.1.102.64 and earlier versions for Windows, Macintosh, Linux, and Solaris. These vulnerabilities could cause the application to crash and could potentially allow an attacker to take control of the affected system. Adobe recommends users of Adobe Flash Player 10.1.102.64 and earlier versions for Windows, Macintosh, Linux, and Solaris update to Adobe Flash Player 10.2.152.26. Adobe Security Bulletin [APSB11-02](#) provides more details of the vulnerabilities.

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 e-mail 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>