



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary - January 2010 -

This report summarizes general activity as well as updates made to the [National Cyber Alert System](#) for January 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 January 2010, US-CERT issued 15 Current Activity entries, four (4) Technical Cyber Security Alerts, three (3) Cyber Security Alerts, four (4) weekly Cyber Security Bulletins, and two (2) Cyber Security Tips.

Highlights for this month include updates released by Microsoft, Adobe, Apple, Oracle, VMware, and Cisco, along with scams related to the Haitian earthquake disaster and the Internal Revenue Service (IRS).

Contents

Executive Summary	1
Current Activity	1
Technical Cyber Security Alerts	3
Cyber Security Alerts	3
Cyber Security Bulletins	3
Cyber Security Tips	4
Security Highlights	4
Contacting US-CERT	5

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 January 2010	
January 7	Microsoft Releases Advance Notification for January Security Bulletin
January 7	PowerDNS Recursor Update Addresses Multiple Vulnerabilities
January 8	VMware Releases Multiple Updates for ESX
January 12	Adobe Releases Update for Adobe Reader and Acrobat
January 12	Oracle Releases Critical Patch Update for January 2010
January 12	Microsoft Releases January Security Bulletin
January 13	IRS Warns of Online Scams

Current Activity for January 2010	
January 14	Microsoft Releases Security Advisory 979352
January 14	Haitian Earthquake Disaster Email Scams and Search Engine Poisoning Campaigns
January 20	Apple Releases Security Update 2010-001
January 20	Adobe Releases Shockwave Player Update
January 21	Microsoft Releases Cumulative Security Update for Internet Explorer
January 22	RealNetworks, Inc. Releases Updates to Address Vulnerabilities
January 26	Google Releases Chrome 4.0.249.78
January 28	Cisco Releases Security Advisory for Unified MeetingPlace

- Microsoft released updates for Internet Explorer, Word, and Power Point.
 - [Microsoft Security Bulletin Summary for January 2010](#) addressed a vulnerability that may allow an attacker to execute arbitrary code. An attacker may be able to exploit this vulnerability by convincing a user to view content rendered in a specially crafted Embedded OpenType (EOT) font in an application that can render EOT fonts. Common applications that can render EOT fonts include Microsoft Internet Explorer, Microsoft Office Word, and Microsoft Office PowerPoint.
 - Microsoft released Security Advisory [979352](#) to alert users of a vulnerability in Microsoft Internet Explorer. The advisory indicates that exploitation of this vulnerability may allow an attacker to execute arbitrary code. Microsoft also indicates that it is aware of public, active exploitation of this vulnerability. Additional information about this vulnerability can be found in Vulnerability Note [VU#492515](#). Microsoft later released Security Bulletin [MS10-002](#) as a Cumulative Security Update for Internet Explorer.
- Adobe released multiple updates for Reader, Acrobat, and Shockwave Player.
 - Adobe Security Bulletin [APBS10-02](#) updates Reader and Acrobat to address multiple vulnerabilities. These vulnerabilities affect Adobe Reader 9.2 and earlier versions for Windows, Macintosh, and UNIX and Adobe Acrobat 9.2 and earlier versions for Windows and Macintosh. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition.
 - Adobe Security Bulletin [APSB10-03](#) updates Shockwave Player to address multiple vulnerabilities. These vulnerabilities affect Adobe Shockwave Player 11.5.2.602 and earlier versions for Windows and Macintosh. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code.
- Apple released Security Update [2010-001](#) to address multiple vulnerabilities in a number of applications. These vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition. Additional details are described in Apple article [HT4004](#).
- Oracle released its [Critical Patch Update for January 2010](#) to address 24 vulnerabilities across several products. Additional information can be found in US-CERT Technical Cyber Security Alert [TA10-012A](#). This update contains fixes for Oracle Database, Oracle Application Server, Oracle Applications Suite, PeopleSoft and JD Edwards Suite, BEA Products Suite, and Oracle Primavera Products Suite.

- VMware released three security advisories to update multiple products.
 - Security Advisory [VMSA-2010-0001](#) to address multiple vulnerabilities in ESX Service Console packages for Network Security Services (NSS) and NetScape Portable Runtime (NSPR). Exploitation of these vulnerabilities may allow an attacker to obtain sensitive information, cause a denial-of-service condition, bypass security restrictions, and compromise a vulnerable system.
 - VMware updated the previously released advisories: [VMSA-2009-0014.2](#) that addressed vulnerabilities in the Dynamic Host Configuration Protocol (DHCP), Service Console Kernel, and Java JRE packages for ESX, and [VMSA-2009-0004.3](#) that addressed vulnerabilities in the OpenSSL, BIND, and Vim packages for ESX.
- Cisco released security advisory [cisco-sa-20100127-mp](#) to address multiple vulnerabilities in Unified MeetingPlace. These vulnerabilities may allow a remote, unauthenticated attacker to obtain sensitive information, manipulate configuration data, create unauthorized accounts, operate with elevated privileges, 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.

<i>Technical Cyber Security Alerts for January 2010</i>	
<i>January 12</i>	TA10-012A Oracle Updates for Multiple Vulnerabilities
<i>January 12</i>	TA10-012B Microsoft Windows EOT Font and Adobe Flash Player 6 Vulnerabilities
<i>January 13</i>	TA10-013A Adobe Reader and Acrobat Vulnerabilities
<i>January 21</i>	TA10-021A Microsoft Internet Explorer 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 January 2010</i>	
<i>January 12</i>	SA10-012B Microsoft Windows and Adobe Flash Player 6 Vulnerabilities
<i>January 13</i>	SA10-013A Adobe Reader and Acrobat Vulnerabilities
<i>January 21</i>	SA10-021A Microsoft Internet Explorer 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 (NCSA) / US-CERT. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

Security Bulletins for January 2010	
	SB10-004 Vulnerability Summary for the Week of December 28, 2009
	SB10-011 Vulnerability Summary for the Week of January 4, 2010
	SB10-018 Vulnerability Summary for the Week of January 11, 2010
	SB10-025 Vulnerability Summary for the Week of January 18, 2010

A total of 308 vulnerabilities were recorded in the [NVD](#) during January 2010.

Cyber Security Tips

[Cyber Security Tips](#) are primarily intended for non-technical computer users. The January tips focused on encryption and portable devices. Links to the full versions of these documents are listed below.

Cyber Security Tips for January 2010	
January 14	ST04-019 Understanding Encryption
January 28	ST04-020 Protecting Portable Devices: Data Security

Security Highlights

Haitian Earthquake Disaster Email Scams and Search Engine Poisoning Campaigns

US-CERT would like to warn users of potential email scams and search engine poisoning campaigns that may circulate regarding the Haitian Earthquake disaster. The scam emails may contain links or attachments which may direct users to phishing or malware-laden websites. Fraudulent search engine results may return similar malicious web links to phishing and malware websites.

IRS Warns of Online Scams

US-CERT is aware of reports of tax season phishing scams. The U.S. Internal Revenue Service has issued a [news release](#) on its website warning consumers about potential scams. These scams are circulating via fraudulent email or other online messages appearing to come from the IRS. They attempt to convince consumers to reveal personal and financial information that can be used to gain access to bank accounts, credit cards, and other financial institutions.

US-CERT encourages users to do the following to mitigate the risks:

- Do not follow unsolicited web links received in email messages.
- Maintain up-to-date antivirus software.
- Review the Federal Trade Commission's [Charity Checklist](#).
- Verify the legitimacy of the email by contacting the organization directly through a trusted contact number (see Better Business Bureau [National Charity Report Index](#)).
- Review the [How to Report and Identify Phishing, E-mail Scams and Bogus IRS Web Sites](#) document on the IRS website.
- Refer to the [Recognizing and Avoiding Email Scams](#) (pdf) document for more information on social engineering attacks.
- Refer to the [Avoiding Social Engineering and Phishing Attacks](#) (pdf) document 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 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>