US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary
- January 2011 -

This report summarizes general activity as well as updates made to the National Cyber Alert System in January 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 January 2011, US-CERT issued 16 Current Activity entries, one Technical Cyber Security Alert, one Cyber Security Alert, five weekly Cyber Security Bulletins, and one Cyber Security Tip.

Highlights for this month include updates or advisories released by Microsoft, Oracle, and RealNetworks, and RIM.

Contents

Current Activity

Current Activity entries are high-impact security threats and vulnerabilities presently being 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 January 2011	
January 3	WordPress.org has released WordPress 3.0.4
January 5	Microsoft Releases Security Advisory
January 6	Apple Releases Mac OS X v10.6.6
January 6	Microsoft Releases Advance Notification for January Security Bulletin
January 7	Microsoft Internet Explorer 8 use-after-free Vulnerability
January 11	Microsoft Releases January Security Bulletin
January 12	Microsoft Security Advisory 2488013
January 12	RIM Releases Security Advisory for BlackBerry Enterprise Server
January 14	Google Releases Chrome 8.0.552.237
January 19	Oracle Releases Critical Patch Update for January 2011

Current Activity for January 2011	
January 28	Microsoft Releases Security Advisory 2501696
January 28	RealNetworks, Inc. Releases Update for RealPlayer
January 28	Opera 11.01 Released

- Apple released Mac OS X v10.6.6 to address a vulnerability affecting PackageKit. Exploitation of this vulnerability may allow an attacker to execute arbitrary code or cause a denial-of-service condition.
- Google released Chrome 8.0.552.237 for all platforms to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition.
- Opera released version 11.01 of the Opera web browser for Windows, MAC, and Unix to address multiple vulnerabilities. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, bypass security restrictions, or obtain sensitive information.
- RealNetworks released updates for Windows RealPlayer 14.0.1 and prior to address a vulnerability. Exploitation of this vulnerability may allow an attacker to execute arbitrary code.
- RIM released security advisory KB25382 to address vulnerability in the PDF distiller of the BlackBerry Enterprise Server. Execution of arbitrary code or a denial-of-service condition may result from this vulnerability.
- Microsoft released three security advisories and a bulletin.
  - Microsoft released security advisory 2490606 to alert users of a vulnerability affecting Windows Graphics Rendering Engine. Attackers may install programs, view, change, or delete data, or even create new accounts with full user rights if the vulnerability is exploited.
  - Microsoft Security Advisory 2488013 addressed a vulnerability in Internet Explorer. This advisory was updated to include Microsoft Fix It 50591 which prevented the recursive loading of CSS style sheets in Internet Explorer as mitigation. Exploitation of this vulnerability may allow an attacker to execute arbitrary code.
  - Microsoft security advisory 2501696 was released to indicate that it was investigating public reports of a vulnerability affecting Windows. This vulnerability was due to the way MHTML interprets MIME-formatted requests for content blocks within a document. Exploitation of this vulnerability may allow an attacker to obtain sensitive information.
  - Updates to address vulnerabilities in MS Windows were released as a part of the MS Bulletin Summary for January 2011. Exploitation of the vulnerabilities may allow an attacker to execute arbitrary code.
- WordPress.org released WordPress 3.0.4 to address a vulnerability in the HTML sanitation library. Exploitation may allow an attacker to insert arbitrary HTML and script code into the browser session.

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 January 2011	
January 11	TA11-011A 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.

Cyber Security Alerts (non-technical) for January 2011	
January 11	SA11-011A 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 (NCSD) / US-CERT. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

Security Bulletins for January 2011
SB11-003 Vulnerability Summary for the Week of December 27, 2010
SB11-010 Vulnerability Summary for the Week of January 3, 2011
SB11-017 Vulnerability Summary for the Week of January 10, 2011
SB11-024 Vulnerability Summary for the Week of January 17, 2011
SB11-031 Vulnerability Summary for the Week of January 24, 2011

A total of 396 vulnerabilities were recorded in the NVD during January 2011.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users. The focus of January's tip regarded the popularity of online shopping and the unique risks presented by the Internet.

Cyber Security Tips for January 2011	
January 26	ST06-003 Staying Safe on Social Network Sites

Security Highlights

Microsoft Internet Explorer 8 Use-After-Free Vulnerability

Microsoft Internet Explorer 8 was found susceptible to a use-after-free vulnerability due to improper handling of circular memory references. Attackers can cause the user's browser to crash and possibly execute arbitrary code as the actual user. No practical solution to the problem is currently available. Users should take full advantage of mitigations found in Microsoft's Enhanced Mitigation Experience Toolkit.

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