



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary - April 2011 -

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

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

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	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 April 2011	
April 1	RealNetworks, Inc. Releases Update for Helix Server and Helix Mobile Server
April 6	WordPress Releases Version 3.1.1
April 8	Microsoft Releases Advance Notification for April Security Bulletin
April 8	ISC dhclient Vulnerability
April 11	VideoLAN Issues Security Advisory
April 12	Microsoft Releases April Security Bulletin
April 15	Adobe Releases Security Advisory for Flash Player, Reader, and Acrobat
April 15	Apple Releases Security Updates
April 15	Oracle Critical Patch Update Pre-Release Announcement
April 15	Google Releases Chrome 10.0.648.205

Current Activity for April 2011	
April 19	Oracle Releases Critical Patch Update for April 2011
April 19	Apple Releases iTunes 10.2.2
April 22	Adobe Releases Security Updates for Reader and Acrobat
April 27	WordPress Releases Version 3.1.2
April 28	Cisco Releases Security Advisory for Cisco Unified Communications Manager
April 28	Google Releases Chrome 11.0.696.57
April 29	Video Game Phishing
April 29	Mozilla Releases Firefox updates

- The [Microsoft Security Bulletin Summary for April 2011](#) provided updates to address vulnerabilities in Microsoft Windows, Internet Explorer, Office, Server Software, and Developer Tools. These vulnerabilities may allow an attacker to execute arbitrary code or operate with elevated privileges.
- Apple released multiple updates for the following products:
 - [Security Update 2011-002](#) addressed a vulnerability in the Certificate Trust Policy for Mac OS X v10.5.8, Mac OS X Server v10.5.8, Mac OS X v10.6.7, and Mac OS X Server v10.6.7. Exploitation of this vulnerability may allow an attacker to intercept user credentials, or obtain sensitive information.
 - [Safari 5.0.5](#) addressed two vulnerabilities affecting the WebKit package that may allow an attacker to execute arbitrary code or cause a denial-of-service condition.
 - [iOS 4.2.7 Software Update for iPhone](#) addressed multiple vulnerabilities affecting the Certificate Trust Policy, QuickLook, and WebKit packages. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service (DoS) condition, intercept user credentials, or obtain sensitive information.
 - [iOS 4.3.2 Software Update](#) addresses multiple vulnerabilities affecting the Certificate Trust Policy, libxslt, QuickLook, and WebKit. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code, cause a DoS condition, intercept user credentials, obtain sensitive information, or bypass security restrictions.
 - iTunes 10.2.2 addressed multiple vulnerabilities affecting the WebKit package that may allow an attacker to execute arbitrary code or cause a DoS condition. Review Apple article [HT4609](#) for additional details.
- Adobe released security updates for Adobe Flash Player, Reader, and Acrobat to address the vulnerability previously referenced in Adobe Security Advisory [APSA11-02](#). Exploitation of this vulnerability may allow an attacker to execute arbitrary code or cause a denial-of-service condition. Adobe indicated that this vulnerability was being exploited in targeted attacks via a Flash (.swf) file embedded in a Microsoft Word (.doc) or Microsoft Excel (.xls) file delivered as an email attachment. US-CERT encourages users and administrators to review Adobe security bulletins [APSB11-07](#) and [APSB11-08](#) and apply any necessary updates to help mitigate the risks.
- Google released two updates for the Chrome Web browser in April 2011. The updates addressed vulnerabilities that enabled attackers to execute arbitrary code, conduct cross-site scripting attacks, or exploit Adobe Flash. The latest version released was Chrome 11.0.696.57.

- Mozilla released Firefox 4.0.1, 3.6.17, and 3.5.19 to address multiple vulnerabilities. The impact of these vulnerabilities includes arbitrary code execution, privilege escalation, directory traversal, and information disclosure. US-CERT encourages users and administrators to review the [Mozilla Foundation Security Advisories](#) for April 28, 2011 and apply any necessary updates to mitigate the risks.
- Cisco released a security advisory to address multiple vulnerabilities in Cisco Unified Communications Manager. These vulnerabilities may allow an attacker to perform SQL injection attacks, conduct directory traversal attacks, or cause a denial-of-service condition. US-CERT encourages users and administrators to review Cisco security advisory [cisco-sa-20110427-cucm](#) and apply any necessary updates or workarounds to help mitigate the risks.

Technical Cyber Security Alerts

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

Technical Cyber Security Alerts for April 2011	
April 12	TA11-102A Microsoft Updates for Multiple Vulnerabilities

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.

Cyber Security Alerts (non-technical) for April 2011	
April 12	SA11-102A 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 April 2011	
	SB11-094 Vulnerability Summary for the Week of March 28, 2011
	SB11-101 Vulnerability Summary for the Week of April 4, 2011
	SB11-108 Vulnerability Summary for the Week of April 11, 2011
	SB11-115 Vulnerability Summary for the Week of April 18, 2011

A total of 312 vulnerabilities were recorded in the NVD during April 2011.

Cyber Security Tips

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

Cyber Security Tips for April 2011	
April 7	ST06-004 Avoiding the Pitfalls of Online Trading
April 28	ST08-001 Using Caution with USB Drives

Security Highlights

Multiple Web Browser Updates

Updates were released for Apple Safari, Microsoft Internet Explorer, Google Chrome, and Mozilla Firefox this month. Given the prevalence of Web browser vulnerabilities and attempts to exploit them, US-CERT recommends users review and implement these updates.

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>