



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary - April 2009 -

This report summarizes general activity as well as updates made to the [National Cyber Alert System](#) for April 2009. This 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 2009, US-CERT issued 16 Current Activity entries, two (2) Technical Cyber Security Alerts, one (1) Cyber Security Alert, four (4) weekly Cyber Security Bulletins, and one (1) Cyber Security Tip.

Highlights for this month included updates released by Microsoft, Mozilla, Oracle, Adobe, and phishing campaigns involving the tax season and the spread of H1N1 (swine flu).

Contents

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

Current Activity

[Current Activity](#) entries are high-impact types of security incidents currently being reported to US-CERT. This month's highlights and activity are listed below.

- Microsoft (MS) released security advisory [969136](#) for MS Office PowerPoint. By convincing a user to open a specially crafted Office file, a remote attacker may be able to gain access to the affected system with the same rights as the user running PowerPoint.
- Microsoft also released updates to address vulnerabilities in Microsoft Windows, Office, Internet Explorer, and Forefront Edge Security as part of the Microsoft Security Bulletin Summary for [April 2009](#). These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, or operate with escalated privileges.
- Mozilla Foundation released [Firefox 3.0.9](#) and [Firefox 3.0.10](#) in April. Firefox 3.0.9 addressed multiple vulnerabilities that could allow an attacker to execute arbitrary code, leverage additional attacks, or obtain sensitive information. Firefox 3.0.10 addressed a memory corruption vulnerability. Exploitation of this vulnerability may result in a denial-of-service condition. The Mozilla Foundation security advisories indicate that many of these vulnerabilities also affect SeaMonkey and Thunderbird.

- Cisco released security advisory [cisco-sa-20090408-asa](#) to address multiple vulnerabilities in the ASA Adaptive Security Appliance and PIX Security Appliances. These vulnerabilities may allow an attacker to bypass authentication mechanisms, bypass access control lists, or cause a denial-of-service condition.
- Oracle released the [Critical Patch Update for April 2009](#) to address 43 vulnerabilities across several products. This update contains the following security fixes:
 - 16 updates for Oracle Database Server
 - 12 updates for Oracle Application Server
 - 3 updates for Oracle Applications
 - 4 updates for Oracle PeopleSoft and JDEdwards Suite
 - 8 updates for BEA Products Suite
- Public reports emerged regarding two vulnerabilities affecting Adobe Reader and Acrobat. The JavaScript methods customDictionaryOpen() and getAnnots() do not safely handle specially crafted arguments and can be manipulated to execute arbitrary code. Additional information regarding these vulnerabilities can be found in the Adobe PSIRT [blog entry](#) and in the [Vulnerability Notes Database](#).
- As reported for the past two months, the Conficker Worm continues to target Microsoft Windows systems. On April 9, researchers discovered a new variant of the Conficker Worm. This variant updates earlier infections via its peer to peer (P2P) network and resumes scan-and-infect activity against unpatched systems. Public reporting indicates that this variant attempts to download additional malicious code onto victim systems, possibly including copies of the Waledac Trojan, a spam-oriented malicious application which has previously propagated only via bogus email messages containing malicious links.

Current Activity for April 2009	
April 3	Microsoft Releases Security Advisory 969136
April 8	Cisco Releases Security Advisory for ASA Adaptive Security Appliance and PIX Security Appliances
April 9	Conficker Worm Targets Microsoft Windows Systems
April 9	Microsoft Releases Advance Notification for April Security Bulletin
April 14	US Tax Season and Phishing Scams
April 14	Microsoft Releases April Security Bulletin Summary
April 15	Oracle Releases Critical Patch Update for April 2009
April 20	Research In Motion Releases Advisory for BlackBerry PDF Distiller Vulnerabilities
April 22	Mozilla Foundation Releases Firefox 3.0.9
April 27	Swine Flu Phishing Attacks and Email Scams
April 28	Adobe Reader JavaScript Function Vulnerability
April 28	Mozilla Foundation Releases Firefox 3.0.10

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 April 2009</i>	
April 14	TA09-104A Microsoft Updates for Multiple Vulnerabilities
April 15	TA09-105A Oracle 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 April 2009</i>	
April 14	SA09-104A 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) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

<i>Security Bulletins for April 2009</i>	
	SB09-103 Vulnerability Summary for the Week of April 6, 2009
	SB09-110 Vulnerability Summary for the Week of April 13, 2009
	SB09-117 Vulnerability Summary for the Week of April 20, 2009
	SB09-124 Vulnerability Summary for the Week of April 27, 2009

A total of 567 vulnerabilities were recorded in the [NVD](#) during April 2009.

Cyber Security Tips

[Cyber Security Tips](#) are primarily intended for non-technical computer users and are issued every two weeks. April's tip focused on staying safe on social networking sites.

<i>Cyber Security Tips for April 2009</i>	
April 18	ST06-003 Staying Safe on Social Network Sites

Security Highlights

US Tax Season Phishing Scams

In the past, US-CERT has received reports of an increased number of phishing scams that take advantage of the United States tax season. During the April tax deadline, US-CERT received public reports of these scams circulating, and reminded users to remain cautious when receiving unsolicited email that could be potential phishing scams.

Phishing scams may appear as a tax refund, as an offer to assist in filing for a refund, or may contain details about fake e-file websites. These messages may appear to be from the IRS and directly ask users for personal information. These messages may also contain a link and instruct the user to follow the link to a website that requests personal information or contains malicious code.

Swine Flu

Following the publicized spread of the H1N1 (Swine) Flu, [public reports](#) of email scams related to the flu began to circulate. The attacks arrive via unsolicited email messages typically containing a subject line related to the Swine Flu. These email messages may contain a link or an attachment. If users click on this link or open the attachment, they may be directed to a phishing website or exposed to malicious code.

Due to these potential phishing attacks and email scams, US-CERT encourages users to visit the Center for Disease Control (CDC) [website](#) for trusted information regarding the Swine Flu.

US-CERT encourages users to take the following measures to protect themselves from spam and phishing scams:

- Do not follow unsolicited web links or attachments in email messages.
- Maintain up-to-date antivirus software.
- Refer to the [Recognizing and Avoiding Email Scams](#) (pdf) document for more information on avoiding email scams.
- Refer to the [Avoiding Social Engineering and Phishing Attacks](#) 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 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: [CF5B48C2](#)

PGP Key Fingerprint: 01F1 9C58 0817 D612 45ED 3FCF 3004 FE8C CF5B 48C2

PGP Key: <https://www.us-cert.gov/pgp/info.asc>