



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary - April 2010 -

This report summarizes general activity as well as updates made to the [National Cyber Alert System](#) in April 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 April 2010, US-CERT issued 21 Current Activity entries, three (3) Technical Cyber Security Alerts, two (2) Cyber Security Alert, four (4) weekly Cyber Security Bulletins, and one (1) Cyber Security Tip.

Highlights for this month include multiple updates released by Microsoft, Adobe, VMware, Oracle, Cisco, Apple, and McAfee, along with web browser updates from Mozilla, Google, Opera, and Sun.

Contents

| | |
|--|----------|
| Executive Summary | 1 |
| Current Activity | 1 |
| Technical Cyber Security Alerts | 3 |
| Cyber Security Alerts | 4 |
| Cyber Security Bulletins | 4 |
| 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 lists all of the entries posted this month followed by a brief overview of the most significant entries.

| Current Activity for April 2010 | |
|--|---|
| April 2 | Mozilla Releases Firefox V3.6.3 |
| April 2 | VMware Releases Security Advisory for ESX Service Console Updates |
| April 5 | Foxit Reader 3.2.1.0401 Released |
| April 7 | Adobe Releases Guidance for Launch Functionality Mitigation in Acrobat and Reader |
| April 8 | Microsoft Releases Advance Notification for April Security Bulletin |
| April 9 | VMware Releases Security Advisory VMSA-2010-0007 |
| April 13 | Adobe Releases Security Updates for Adobe Reader and Acrobat |

| Current Activity for April 2010 | |
|--|--|
| April 13 | Microsoft Releases April Security Bulletin |
| April 13 | Sun Java Deployment Toolkit Plugin and ActiveX Control Vulnerability |
| April 14 | Oracle Releases Critical Patch Update for April 2010 |
| April 15 | Cisco Releases Security Advisory |
| April 15 | Apple Releases Security Update 2010-003 |
| April 16 | Oracle Releases Sun Java SE 1.6.0_20 |
| April 21 | Google Releases Chrome 4.1.249.1059 |
| April 22 | McAfee DAT 5958 Issues |
| April 22 | VideoLAN Releases Security Advisory for VLC Media Player |
| April 22 | Cisco Releases Security Advisory for Small Business Video Surveillance Cameras and 4-Port Gigabit Security Routers |
| April 23 | Microsoft Revokes Security Update |
| April 27 | Microsoft Re-Releases Security Update for MS10-025 |
| April 28 | Google Releases Chrome 4.1.249.1064 |
| April 30 | Opera Software Releases Opera 10.53 |

- Microsoft released updates for Microsoft Windows, Office, Exchange, and Windows Media Services.
 - The Microsoft Security Bulletin Summary for [April 2010](#) addressed vulnerabilities in Microsoft Windows, Office, and Exchange. These vulnerabilities may allow an attacker to execute arbitrary code, operate with elevated privileges, cause a denial-of-service attack, or spoof an IPv4 address to bypass filtering devices.
 - Microsoft re-released a security update related to Microsoft security bulletin [MS10-025](#), which addressed a vulnerability in Windows Media Services running on Windows 2000 Server. The original release of this update had been revoked because it did not effectively correct the underlying vulnerability. Additional information can be found in the Microsoft Security Response Center [blog](#).
- Adobe posted a blog entry and security bulletin to address vulnerabilities in Acrobat and Reader.
 - Adobe released a [blog entry](#) to address a vulnerability in Acrobat and Reader that exists due to the way Adobe Acrobat and Adobe Reader handle launch actions embedded in PDFs. An attacker may be able to manipulate the content in the file name section of the dialog box to trick users into opening a malicious PDF.
 - Security bulletin [APSB10-09](#) addressed several vulnerabilities in multiple versions of Adobe Reader and Acrobat.
- VMware released two security advisories to address multiple vulnerabilities that affected multiple products.
 - Security advisory [VMSA-2010-0006](#) addressed vulnerabilities in the Samba and acpid packages of ESX Service Console. These vulnerabilities may allow an attacker to cause a denial-of-service condition, obtain sensitive information, or bypass security restrictions.

- Security advisory [VMSA-2010-0007](#) addressed multiple vulnerabilities in VMware hosted products, vCENTER Server, and ESX. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code, operate with elevated privileges, obtain sensitive information, or cause a denial-of-service condition.
- Oracle released a critical patch update and a new version of Sun Java SE.
 - The Oracle [Critical Patch Update for April 2010](#) addressed 47 vulnerabilities across several products. This update contained security fixes for Oracle Database Server, Fusion Middleware, Collaboration Suite, Application Suite, PeopleSoft and JD Edwards Suite, Industry Applications, and the Solaris Products Suite.
 - Sun Java SE 1.6.0_20 addressed several vulnerabilities in Java Deployment Toolkit and the new Java Plug-in. Exploitation of these vulnerabilities may allow a remote, unauthenticated attacker to execute arbitrary code. Additional information can be found in Oracle security alert [CVE-2010-0886](#), Sun Java SE 1.6.0_20 [release notes](#), and US-CERT Vulnerability Note [VU#886582](#). Please note that web browsers using the plug-in version of the Java Deployment Toolkit may not be properly updated.
- Cisco released two security advisories.
 - Security advisory [cisco-sa-20100414-csd](#) addressed a vulnerability in Cisco Secure Desktop, which had a vulnerable ActiveX control that may allow an attacker to execute arbitrary code. Cisco also provided a workaround for users who are unable to apply the update.
 - Security advisory [cisco-sa-20100421-vsc](#) addressed a vulnerability that affects Cisco Small Business Video Surveillance Cameras and Cisco RVS4000 4-Port Gigabit Security Routers. This vulnerability may allow an unprivileged user to gain full administrative access on the device or obtain sensitive information.
- Apple released security update 2010-003 to address a vulnerability in the Apple Type Services (ATS) package. This vulnerability may allow an attacker to execute arbitrary code. Additional information can be found in Apple article [HT4131](#).
- McAfee's VirusScan software DAT release 5958 incorrectly identified the valid Microsoft Windows system file, C:\Windows\system32\svchost.exe, as containing malicious code. Symptoms include a denial-of-service condition when the McAfee software attempts to clean the file. Corporate users and administrators are encouraged to review the McAfee Corporate Knowledgebase Article [KB68780](#), while home users are encouraged to review the McAfee FAQ Document [TS100969](#).

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 April 2010 | |
|---|--|
| April 13 | TA10-103A Microsoft Updates for Multiple Vulnerabilities |
| April 13 | TA10-103B Oracle Updates for Multiple Vulnerabilities |
| April 13 | TA10-103C Adobe Reader and Acrobat 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 April 2010 | |
|---|--|
| April 13 | SA10-103A Microsoft Updates for Multiple Vulnerabilities |
| April 13 | SA10-103C Adobe Reader and Acrobat 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 2010 |
|---|
| SB10-095 Vulnerability Summary for the Week of March 29, 2010 |
| SB10-102 Vulnerability Summary for the Week of April 5, 2010 |
| SB10-109 Vulnerability Summary for the Week of April 12, 2010 |
| SB10-116 Vulnerability Summary for the Week of April 19, 2010 |

A total of 501 vulnerabilities were recorded in the [NVD](#) during April 2010.

Cyber Security Tips

[Cyber Security Tips](#) are primarily intended for non-technical computer users. The April tip focused on copyright infringement. A link to the full version of the document is listed below.

| Cyber Security Tips for April 2010 | |
|---|--|
| April 28 | ST05-004 Avoiding Copyright Infringement |

Security Highlights

Web Browsers and Java Plugin Updates

Mozilla Firefox

The Mozilla Foundation released Firefox V3.6.3 to address a critical vulnerability. Exploitation of this vulnerability may allow an attacker to execute arbitrary code. Additional information can be found in Mozilla Foundation Security Advisory [mfsa2010-25](#).

Google Chrome

Google released two updates for the Chrome web browser. Chrome 4.1.249.1059 was released for Microsoft Windows to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code, conduct cross-site scripting attacks, or conduct cross-site request forgery

attacks. Additional information can be found in the Google Chrome Releases [blog entry](#) for April 20, 2010.

Google later released Chrome 4.1.249.1064, also for Microsoft Windows, to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code or bypass the same origin policy in the browser. US-CERT encourages users and administrators to review the Google Chrome Releases [blog entry](#) for April 27, 2010, and update to Chrome 4.1.249.1064 for Windows to help mitigate the risks.

Opera

Opera Software released [Opera 10.53](#) to address a vulnerability that impacts Opera for Windows and Mac OS X. According to Opera, this vulnerability is extremely severe and allows multiple asynchronous document modifications to be used to execute arbitrary code. US-CERT encourages users and administrators to review the Opera Software [security advisory](#) related to this vulnerability and upgrade to [Opera 10.53](#) to help mitigate the risks.

Sun Java Development Toolkit

The Sun Java Development Toolkit plugin and ActiveX control contain a vulnerability. This vulnerability is due to insufficient argument validation. By convincing a user to visit a specially crafted HTML document, an attacker may be able to exploit this vulnerability and execute an arbitrary JAR file on the affected system. US-CERT encourages users and administrators to review US-CERT Vulnerability Note [VU#886582](#) and implement any necessary workarounds to help mitigate the risk until a fix is available from the product vendor.

In addition, users and administrators should review and implement the best security practices to help prevent future, similar attacks as described in the [Securing Your Web Browser](#) document and Security Tip [ST04-012](#) - Understanding Active Content and Cookies.

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>