



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary - May 2010 -

This report summarizes general activity as well as updates made to the [National Cyber Alert System](#) in May 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 May 2010, US-CERT issued nine (9) Current Activity entries, one (1) Technical Cyber Security Alerts, one (1) Cyber Security Alert, four (4) weekly Cyber Security Bulletins, and two (2) Cyber Security Tips.

Highlights for this month include updates released by Microsoft, Apple, Cisco, Adobe, Google, and Foxit.

Contents

Executive Summary.....	1
Current Activity.....	1
Technical Cyber Security Alerts.....	2
Cyber Security Alerts.....	3
Cyber Security Bulletins.....	3
Cyber Security Tips.....	3
Security Highlights.....	3
Contacting US-CERT.....	4

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 May 2010	
May 5	Foxit Releases Foxit Reader 3.3
May 7	Microsoft Releases Advance Notification for May Security Bulletin
May 10	Apple Safari Vulnerability
May 11	Microsoft Releases May Security Bulletin
May 12	Adobe Releases Update for Shockwave Player
May 13	Cisco Releases Updates for PGW Softswitch
May 19	Apple Releases Updates for Java Mac OS X 10.5 and 10.6
May 26	Google Releases Chrome 5.0.375.55
May 27	Cisco Network Building Manager Vulnerabilities

- Microsoft released updates to address vulnerabilities in Microsoft Windows, Office, and Visual Basic for Applications as part of the [Microsoft Security Bulletin Summary for May 2010](#). These vulnerabilities may allow an attacker to execute arbitrary code.
- Apple released updates for the Safari web browser and Java for Mac OS X.
 - Exploit code for an Apple Safari web browser vulnerability was publicly released. By convincing a user to open a specially crafted web page, an attacker may be able to execute arbitrary code. This issue can be mitigated by disabling JavaScript in Apple Safari. Apple released Safari 5.0 and 4.1 in June to address multiple vulnerabilities.
 - Apple released Java for Mac OS X 10.5 Update 7 and Java for Mac OS X 10.6 Update 2 to address multiple vulnerabilities that may allow an attacker to execute arbitrary code or cause a denial-of-service condition. Additional details are described in Apple Article [HT4170](#) and [HT4171](#).
- Cisco released updates for PGW Softswitch and Network Building Manager.
 - Cisco released security advisory [cisco-sa-20100512-pgw](#) to address multiple vulnerabilities in Cisco PGW Softswitch. These vulnerabilities may allow an attacker to cause a denial-of-service condition.
 - Cisco released security advisory [cisco-sa-20100526-mediator](#) to address multiple vulnerabilities in Network Building Manager. The advisory indicated that the legacy Richards-Zeta Mediator products were also affected by these vulnerabilities. Exploitation of these vulnerabilities may allow an attacker to operate with escalated privileges or obtain sensitive information.
- Adobe released a security update to address multiple vulnerabilities in Adobe Shockwave Player 11.5.6.606 and earlier versions for both Windows and Macintosh operating systems. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code. Additional details are provided in Adobe security bulletin [APSB10-12](#).
- Google released [Chrome 5.0.375.55](#) for Linux, Mac, and Windows to address multiple vulnerabilities. These vulnerabilities may allow an attacker to bypass security restrictions, execute script in an unsafe context, or mislead users.
- The Foxit Corporation released Foxit Reader 3.3 for Windows. This update addresses a /Launch function vulnerability in the Foxit Reader. Additional information regarding the /Launch function vulnerability can be found in the [Vulnerability Notes entry VU#570177](#).

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 May 2010</i>	
May 11	TA10-131A 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.

<i>Cyber Security Alerts (non-technical) for May 2010</i>	
<i>May 11</i>	SA10-131A 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.

<i>Security Bulletins for May 2010</i>
SB10-123 Vulnerability Summary for the Week of April 26, 2010
SB10-130 Vulnerability Summary for the Week of May 3, 2010
SB10-137 Vulnerability Summary for the Week of May 10, 2010
SB10-144 Vulnerability Summary for the Week of May 17, 2010

A total of 420 vulnerabilities were recorded in the [NVD](#) during May 2010.

Cyber Security Tips

[Cyber Security Tips](#) are primarily intended for non-technical computer users. The May tip focused on end-user license agreements and file-sharing technology.

<i>Cyber Security Tips for May 2010</i>	
<i>May 5</i>	ST05-005 Reviewing End-User License Agreements
<i>May 19</i>	ST05-007 Risks of File-Sharing Technology

Security Highlights

The Foxit Corporation released Foxit Reader 3.3 for Windows. [Foxit Reader](#) is software designed to view Portable Document Format (PDF) files. This update addressed a vulnerability in the PDF specification /Launch function.

Foxit Reader uses the [ShellExecute](#) function to handle PDFs that use a Launch action. In some cases, Foxit Reader would not prompt the user before an application was launched with a Launch action. It was also [reported](#) that the Launch Action can be used to launch an executable that is included in the PDF document, which resulted in arbitrary code execution. By convincing a user to open a specially crafted PDF document (e.g., by visiting a website) a remote, unauthenticated attacker may be able to execute arbitrary code on a vulnerable system.

Foxit Reader 3.3 contains a component called Trust Manager. The Foxit Reader release notes indicated that the Trust Manager enabled users to allow or deny unauthorized actions and data transmission, including URL connection, attachments PDF action, and JavaScript. This update will cause Foxit Reader to prompt the user before using a Launch Action.

Additional information regarding the /Launch function vulnerability can be found in the [Vulnerability Notes entry VU#570177](#).

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>