



# US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

## Monthly Activity Summary - June 2011 -

This report summarizes general activity including updates to the [National Cyber Alert System](#) in June 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 June 2011, US-CERT issued 21 Current Activity entries, two Technical Cyber Security Alerts, two Cyber Security Alerts, four weekly Cyber Security Bulletins, and one Cyber Security Tip.

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

### Contents

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

### 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.

<b>Current Activity for June 2011</b>	
<b>June 1</b>	<a href="#">Apple Releases Malware Detection Tool</a>
<b>June 2</b>	<a href="#">Gmail Phishing Attack</a>
<b>June 2</b>	<a href="#">Cisco Releases Security Advisories for Multiple Products</a>
<b>June 6</b>	<a href="#">VMware Releases Security Advisory</a>
<b>June 6</b>	<a href="#">Adobe Releases Security Update for Flash Player</a>
<b>June 6</b>	<a href="#">Oracle Issues Pre-Release Announcement for June 2011</a>
<b>June 6</b>	<a href="#">VideoLAN Releases VLC Media Player 1.1.10</a>
<b>June 8</b>	<a href="#">Google Chrome Releases 12.0.742.91</a>
<b>June 8</b>	<a href="#">Oracle Releases Critical Patch Update for June 2011</a>
<b>June 9</b>	<a href="#">Microsoft Releases Advance Notification for June Security Bulletin</a>

<b>Current Activity for June 2011</b>	
<b>June 10</b>	<a href="#">Adobe Prenotification Security Advisory for Adobe Reader and Acrobat</a>
<b>June 14</b>	<a href="#">Microsoft Releases June Security Bulletin</a>
<b>June 15</b>	<a href="#">Adobe Releases Security Bulletin for Critical Vulnerability in Flash Player</a>
<b>June 15</b>	<a href="#">Adobe Releases Security Bulletin for Adobe Reader and Acrobat</a>
<b>June 15</b>	<a href="#">Adobe Releases Security Bulletin for Critical Vulnerabilities in Shockwave Player</a>
<b>June 21</b>	<a href="#">RIM Releases Security Advisory for BlackBerry PlayBook</a>
<b>June 22</b>	<a href="#">Mozilla Releases Firefox 5 and 3.6.18</a>
<b>June 24</b>	<a href="#">Apple Releases Security Updates to Address Multiple Vulnerabilities</a>
<b>June 28</b>	<a href="#">Google Releases Chrome 12.0.742.112</a>
<b>June 29</b>	<a href="#">Apple Releases Java Updates for Mac OS X 10.5 and OS X 10.6</a>
<b>June 30</b>	<a href="#">WordPress Releases Version 3.1.4</a>

- The [Microsoft Security Bulletin Summary for June 2011](#) provided updates to address vulnerabilities in Microsoft Windows, Microsoft Office, Microsoft SQL Server, Microsoft Visual Studio, Microsoft .NET framework, Microsoft Silverlight, Microsoft Forefront Threat Management Gateway, and Internet Explorer. These vulnerabilities may allow an attacker to execute arbitrary code, obtain sensitive information, or cause a denial-of-service condition.
- Apple released security updates, a malware detection tool, and Java updates:
  - Mac OS X 10.6.8 and Security Update 2011-004 addressed multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code, disclose sensitive information, or cause a denial-of-service condition. Further information on these updates can be found in Apple Support Article [HT4723](#).
  - Apple released [Security Update 2011-003](#) for Mac OS X in response to the recent Mac fake antivirus software. The update adds a malware definition to the File Quarantine application, causes the File Quarantine application to automatically update its malware definition list daily, and removes the MacDefender fake antivirus software if detected.
  - [Java for Mac OS X 10.5 Update 10](#) and [Java for Mac OS X 10.6 Update 5](#) addressed multiple vulnerabilities which may allow an attacker to execute arbitrary code.
- Adobe released updates for Flash Player, Reader, Acrobat, and Shockwave Player to address multiple vulnerabilities. These vulnerabilities affect:
  - Flash Player 10.3.181.16 and earlier versions for Windows, Macintosh, Linux, and Solaris
  - 10.3.185.22 and earlier versions for Android
  - Adobe Flash Player 10.3.181.23 and earlier for Windows, Macintosh, Linux, and Solaris
  - Adobe Flash Player 10.3.185.23 and earlier for Android
  - Adobe Reader 10.0.1 and earlier versions for Windows
  - Adobe Reader 10.0.3 and earlier versions of Macintosh
  - Adobe Acrobat 10.0.3 and earlier versions for Windows and Macintosh
  - Adobe Shockwave Player 11.5.9.620 and earlier versions on the Windows and Macintosh operating systems

Exploitation of these vulnerabilities may allow an attacker to cause a denial-of-service condition, conduct a cross-site scripting attack, or execute arbitrary code. US-CERT encourages users and

administrators to review Adobe Security Advisories [APSB11-13](#), [APSB11-16](#), [APSB11-17](#), and [APSB11-18](#) and apply any necessary updates to help mitigate the risks.

- Google released two updates for the Chrome Web browser in June 2011. The updates addressed vulnerabilities that enabled attackers to execute arbitrary code. The latest version released was Chrome 12.0.742.112, which also contains an updated version of Flash.
- Mozilla released Firefox 5 and Firefox 3.6.18 to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code, violate the same origin policy, or perform a cross-site scripting attack.
- Cisco released security advisories for Cisco Unified IP phones, Cisco Network Registrar, Cisco AnyConnect Secure Mobility Client, and Cisco Media Experience to address multiple vulnerabilities. Exploitation of the vulnerabilities may allow an attacker to execute arbitrary code, operate with escalated privileges, or gain administrative access.

### **Technical Cyber Security Alerts**

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

<i>Technical Cyber Security Alerts for June 2011</i>	
<b>June 14</b>	<a href="#">TA11-165A Microsoft Updates for Multiple Vulnerabilities</a>
<b>June 15</b>	<a href="#">TA11-166A Adobe Updates for Multiple Vulnerabilities</a>

### **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.

<i>Cyber Security Alerts (non-technical) for June 2011</i>	
<b>June 14</b>	<a href="#">SA11-165A Microsoft Updates for Multiple Vulnerabilities</a>
<b>June 15</b>	<a href="#">SA11-166A Adobe Updates for Multiple Vulnerabilities</a>

### **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>Cyber Security Bulletins for June 2011</i>	
<b>June 6</b>	<a href="#">SB11-157 Vulnerability Summary for the Week of May 30, 2011</a>
<b>June 13</b>	<a href="#">SB11-164 Vulnerability Summary for the Week of June 6, 2011</a>
<b>June 20</b>	<a href="#">SB11-171 Vulnerability Summary for the Week of June 13, 2011</a>
<b>June 27</b>	<a href="#">SB11-178 Vulnerability Summary for the Week of June 20, 2011</a>

A total of 294 vulnerabilities were recorded in the NVD during June 2011.

## **Cyber Security Tips**

[Cyber Security Tips](#) are primarily intended for non-technical computer users. The focus of June's tip was cyberbullying.

<b>Cyber Security Tips for June 2011</b>	
<b>June 1</b>	<a href="#">ST06-005 Dealing with Cyberbullies</a>

## **Security Highlights**

### **Microsoft Releases June Security Bulletin**

Microsoft has released updates to address vulnerabilities in Microsoft Windows, Microsoft Office, Microsoft SQL Server, Microsoft Visual Studio, Microsoft .NET framework, Microsoft Silverlight, Microsoft Forefront Threat Management Gateway, and Internet Explorer as part of the [Microsoft Security Bulletin Summary for June 2011](#). These vulnerabilities may allow an attacker to execute arbitrary code, obtain sensitive information, or cause a denial-of-service condition.

US-CERT encourages users and administrators to review the [Bulletin](#) and apply any necessary updates to help mitigate the risks.

## **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](mailto:info@us-cert.gov).

Web Site Address: <http://www.us-cert.gov>

E-mail Address: [info@us-cert.gov](mailto: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>