



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary - May 2009 -

This report summarizes general activity as well as updates made to the [National Cyber Alert System](#) for May 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 May 2009, US-CERT issued 21 Current Activity entries, three (3) Technical Cyber Security Alerts, three (3) Cyber Security Alerts, four (4) weekly Cyber Security Bulletins, and one (1) Cyber Security Tip.

Highlights for this month include updates released by Adobe, Microsoft, Apple, Cisco, NSD DNS, and VMWare; and propagation of the Gumblar malware.

Contents

Executive Summary	1
Current Activity	1
Technical Cyber Security Alerts	2
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 being reported to US-CERT. The most significant entries of the month are highlighted below followed by a table listing all of the entries posted this month.

- Adobe released Security Bulletin [APSB09-05](#) to address a potential vulnerability in versions of Flash Media Server up to and including version 3.5.1. This vulnerability may allow an attacker to "execute remote procedures within a server side ActionScript file running on a Flash Media Server." According to Adobe, this issue affects versions of Flash Media Interactive Server and Flash Media Streaming Server.
- Microsoft released multiple updates in May that included their monthly security bulletin, an advisory on a vulnerability affecting Microsoft Internet Information Services 6 (IIS6), and the release of Service Pack 2 for Windows Vista and Windows Server 2008:
 - Microsoft released an update to address a vulnerability in Microsoft Office as part of the Microsoft Security Bulletin Summary for [May 2009](#). By convincing a user to open a specially crafted PowerPoint file, an attacker may be able to execute arbitrary code. Additional information regarding this vulnerability can be found in Technical Cyber Security Alert [TA09-132A](#).

- Reports identified a vulnerability affecting Microsoft Internet Information Services 6 (IIS6) due to its improper handling of unicode tokens. Exploitation of this vulnerability may allow a remote attacker to bypass authentication methods, allowing the attacker to upload files to a WebDAV folder or obtain sensitive information. US-CERT is also aware of publicly available exploit code and active exploitation of this vulnerability. Additional information regarding this vulnerability can be found in Microsoft Security Advisory [971492](#) and the [Vulnerability Notes Database](#).
- Microsoft also released Service Pack 2 for Windows Vista and Windows Server 2008. This service pack contains multiple security updates and hotfixes. US-CERT encourages users and administrators to review Microsoft Knowledge Base article [948465](#) and follow best-practice security policies to determine if the update should be applied.
- Apple released Security Update 2009-002 and Mac OS X v10.5.7 to address multiple vulnerabilities in a number of applications. These vulnerabilities may allow an attacker to execute arbitrary code, obtain sensitive information, cause a denial-of-service condition, leverage additional attacks, or obtain elevated privileges. Additionally, Apple released Safari 3.2.3 to address vulnerabilities in libxml, Safari, and Webkit. These vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition. These are further described in Apple articles [HT3549](#), [HT3550](#) and in Technical Cyber Security Alert [TA09-133A](#).
- Cisco released a security advisory to address a vulnerability in CiscoWorks TFTP. Exploitation of this vulnerability may allow a remote, unauthenticated attacker to view or modify application and host operating system files, possibly resulting in arbitrary code execution or a denial-of-service condition. The security advisory indicates that multiple Cisco products are affected by this vulnerability. US-CERT encourages users and administrators to review Cisco Security Advisory [cisco-sa-20090520-cw](#) and apply any necessary updates to help mitigate the risks.
- NLnet Labs released a patch to address a vulnerability in NSD DNS versions 2.0.0 through 3.2.1. This vulnerability is due to an error in the way NSD processes certain types of packets that may lead to a buffer overflow. Exploitation of this vulnerability may allow a remote, unauthenticated attacker to cause the DNS software to crash, resulting in a denial-of-service condition. Many system vendors are impacted by this vulnerability. Review the NSD [announcement](#) and the [Vulnerability Notes Database](#) entry for additional information.
- VMware released [Security Advisory VMSA-2009-0007](#) to address multiple vulnerabilities in VMware Workstation, Player, ACE, Server, Fusion, ESX, and ESXi. The first of these vulnerabilities is due to a error in the VMware Descheduled Time Accounting driver. Exploitation of this vulnerability may result in a denial of service in Windows-based virtual machines. The second vulnerability is due to a known error in the libpng package used by some VMware products. Exploitation of this vulnerability may allow an attacker to execute arbitrary code.

Current Activity for May 2009	
May 7	Adobe Releases Security Bulletin for Flash Media Server
May 7	Microsoft Releases Advance Notification for May Security Bulletin
May 13	Microsoft Releases May Security Bulletin
May 13	Apple Releases Security Update 2009-002, Mac OS X v10.5.7 and Safari 3.2.3
May 13	Adobe Releases Security Updates for Adobe Reader and Acrobat
May 18	Gumblar Malware Exploit Circulating
May 19	Microsoft Internet Information Services (IIS) WebDAV Request Vulnerability
May 20	Mac OS X Includes Known Vulnerable Version of Java

Current Activity for May 2009	
May 20	Cisco Releases Security Advisory for CiscoWorks TFTP Vulnerability
May 20	NSD DNS Buffer Overflow Vulnerability
May 22	Novell Releases Updates for GroupWise
May 26	Microsoft Releases Service Pack 2 for Windows Vista and Windows Server 2008
May 27	BlackBerry Security Advisory
May 28	Microsoft Releases Security Advisory 971778
May 29	VMware Releases Security Advisory

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 May 2009	
May 12	TA09-132A Microsoft PowerPoint Multiple Vulnerabilities
May 13	TA09-133A Apple Updates for Multiple Vulnerabilities
May 13	TA09-133B 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 May 2009	
May 12	SA09-132A Microsoft PowerPoint Multiple Vulnerabilities
May 13	SA09-133A Apple Updates for Multiple Vulnerabilities
May 13	SA09-133B 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 (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.

Security Bulletins for May 2009
SB09-124 Vulnerability Summary for the Week of April 27, 2009
SB09-131 Vulnerability Summary for the Week of May 4, 2009
SB09-138 Vulnerability Summary for the Week of May 11, 2009
SB09-146 Vulnerability Summary for the Week of May 18, 2009

A total of 365 vulnerabilities were recorded in the [NVD](#) during May 2009.

Cyber Security Tips

[Cyber Security Tips](#) are primarily intended for non-technical computer users. May's tips focused on cyber security and choosing and protecting passwords.

<i>Cyber Security Tips for May 2009</i>	
May 6	ST04-001 Why is Cyber Security a Problem?
May 21	ST04-002 Choosing and Protecting Passwords

Security Highlights

Propagation of the Gumblar Trojan

Public reports of the Gumblar Trojan malware began circulating in May. This is a drive-by-download exploit that infects systems over multiple stages. The first stage of this exploit attempts to compromise legitimate websites by injecting malicious code into them. Reports indicate these website infections occur primarily through stolen FTP credentials but may also be compromised through poor configuration settings, vulnerable web applications, etc. The second stage of this exploit occurs when users visit a website compromised by Gumblar. Users who visit these compromised websites and have not applied updates for known PDF and Flash Player vulnerabilities may become infected with malware. This malware may be used by attackers to monitor network traffic and obtain sensitive information, including FTP and login credentials, which can be used to conduct further exploits. Additionally, this malware may also redirect Google search results for the infected user.

US-CERT encourages users and administrators to apply software updates in a timely manner and use up-to-date antivirus software to help mitigate the risks.

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>