US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary
- July 2009 -

This report summarizes general activity as well as updates made to the National Cyber Alert System for July 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 July 2009, US-CERT issued 20 Current Activity entries, four (4) Technical Cyber Security Alerts, three (3) Cyber Security Alerts, four (4) weekly Cyber Security Bulletins, and two (2) Cyber Security Tips.

Highlights for this month include multiple updates released by Microsoft, VMware, Mozilla, Cisco, and Adobe.

Contents

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.

- Microsoft released three security advisories, two out-of-band security bulletins, and the July security bulletin:
  - Microsoft has released Security Advisory 972890 to alert users about a vulnerability in Microsoft Video ActiveX Control. Exploitation of this vulnerability may allow an attacker to execute arbitrary code. The advisory also indicates that Microsoft is aware of attacks attempting to exploit the vulnerability. Additional information regarding this vulnerability can be found in Technical Cyber Security Alert TA09-187A.
  - Microsoft released an update to address vulnerabilities in Microsoft Windows, Virtual PC, Virtual Server, ISA Server, and Office as part of the Microsoft Security Bulletin Summary for July 2009. These vulnerabilities may allow an attacker to execute arbitrary code or operate with elevated privileges.

- Microsoft released Security Advisory 973472 to alert users about a vulnerability in Microsoft Office Web Components. Exploitation of this vulnerability may allow a remote attacker to execute arbitrary code. The advisory indicates that Microsoft is aware of attacks attempting to exploit the vulnerability.
- Microsoft released two out-of-band security bulletins. The first bulletin, MS09-034, is a cumulative security update for Internet Explorer that addresses several vulnerabilities. The second bulletin, MS09-035, addresses vulnerabilities in the Visual Studio Active Template Library (ATL). Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code.
- Additionally, Microsoft released security advisory 973882 to provide specific guidance for developers, IT professionals, consumers, and home users regarding the vulnerabilities in Active Template Library (ATL). Additional information can be found in Technical Cyber Security Alert TA09-209A.

- Apple has released Safari 4.0.2, as detailed in Apple article HT3666, to address multiple vulnerabilities in the WebKit component of Safari. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code, conduct cross-site scripting attacks, or cause a denial-of-service condition on Mac OS X and Windows platforms.
- VMware released two security advisories in July:
  - Security advisory VMSA-2009-0009 addressed multiple vulnerabilities involving the udev, sudo, and curl packages of the ESX Service Console, which may allow an attacker to execute arbitrary requests to an affected intranet server, read or overwrite files, or gain elevated privileges on the affected system.
  - Additionally, VMware updated security advisory VMSA-2009-0008.1, which addressed a vulnerability in the krb5 package of the ESX Service Console. Exploitation of this vulnerability may allow an attacker to execute arbitrary code or cause a denial-of-service condition.
- Oracle has released its Critical Patch Update for July 2009 to address 30 vulnerabilities across several products. This update contains security fixes for Database Server, Secure Backup, Application Server, Applications, Enterprise Manager, PeopleSoft and JD Edwards Suite, Siebel Suite, and BEA Products Suite.
- The Mozilla Foundation released Firefox 3.0.12 and 3.5.1 during July.
  - The Mozilla Foundation has released Firefox 3.5.1 to address a vulnerability. This vulnerability is due to an error in the way the Just-in-Time (JIT) compiler returns from native functions. Exploitation of this vulnerability may allow an attacker to execute arbitrary code. Mozilla Foundation Security Advisory 2009-41 and upgrade to Firefox 3.5.1 or apply the suggested workaround provided in the advisory. Additional information can also be found in the Vulnerability Notes Database.
  - The Mozilla Foundation has released Firefox 3.0.12 to address multiple vulnerabilities in Firefox 3.0.x. These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, or launch cross-site-scripting attacks. US-CERT encourages users and administrators to review Mozilla Foundation Security Advisories released on July 21, 2009 and upgrade to Firefox 3.0.12 to help mitigate the risks.

- Cisco released Security Advisory cisco-sa-20090727-wlc to address the following vulnerabilities in Wireless LAN Controllers:
    - Malformed HTTP or HTTPS authentication response denial-of-service vulnerability. SSH connections denial-of-service vulnerability.
    - Crafted HTTP or HTTPS request denial-of-service vulnerability.
    - Crafted HTTP or HTTPS request unauthorized configuration modification vulnerability.

  Exploitation of these vulnerabilities may allow an attacker to cause a denial-of-service condition or gain full control over the Wireless LAN Controller.

Current Activity for July 2009	
July 6	Microsoft Releases Security Advisory 972890
July 9	Microsoft Releases Advance Notification for July Security Bulletin
July 9	FCKeditor Releases Version 2.6.4.1
July 9	Apple Releases Safari 4.0.2
July 10	WordPress Releases Version 2.8.1
July 13	VMware Releases Security Advisory VMSA-2009-0009 and Updates Security Advisory VMSA-2009-0008.1
July 14	Oracle Releases Critical Patch Update for July 2009
July 14	Microsoft Releases July Security Bulletin
July 14	Microsoft Releases Security Advisory 973472
July 17	Mozilla Firefox 3.5 Vulnerability
July 22	Mozilla Releases Firefox 3.0.12
July 22	WordPress Releases Version 2.8.2
July 23	Adobe Reader, Acrobat and Flash Player Vulnerability
July 27	Cisco Releases Security Advisory for Vulnerabilities in Cisco Wireless LAN Controllers
July 27	Microsoft Releases Advance Notification for Out-of-Band Security Bulletins
July 29	Internet Systems Consortium BIND 9 Vulnerability
July 29	Microsoft Releases Two Out-of-Band Security Bulletins and a Security Advisory
July 30	Cisco Releases Security Advisory for IOS Software Vulnerabilities
July 31	Adobe Releases Security Updates for Reader and Acrobat
July 31	Adobe Releases Shockwave Player Update and Flash Player Update

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 July 2009	
July 6	TA09-187A Microsoft Video ActiveX Control Vulnerability
July 14	TA09-195A Microsoft Updates for Multiple Vulnerabilities
July 23	TA09-204A Adobe Flash Vulnerability Affects Flash Player and Other Adobe Products
July 28	TA09-209A Microsoft Windows, Internet Explorer, and Active Template Library (ATL) 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 July 2009	
July 6	SA09-187A Microsoft Video ActiveX Control Vulnerability
July 14	SA09-195A Microsoft Updates for Multiple Vulnerabilities
July 28	SA09-209A Microsoft Windows and Internet Explorer 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 July 2009
SB09-187 Vulnerability Summary for the Week of June 29, 2009
SB09-194 Vulnerability Summary for the Week of July 6, 2009
SB09-201 Vulnerability Summary for the Week of July 13, 2009
SB09-208 Vulnerability Summary for the Week of July 20, 2009

A total of 446 vulnerabilities were recorded in the NVD during July 2009.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users and are issued monthly. July's tip focused on understanding patches.

Cyber Security Tips for July 2009	
July 15	ST04-006 Understanding Patches
July 29	ST04-007 Reducing Spam

Security Highlights

Adobe Updates Reader, Acrobat, Flash, and Shockwave

Multiple updates were released by Adobe for Reader, Acrobat, Flash, and Shockwave to address multiple vulnerabilities. By convincing a user to open a PDF document embedded with a specially crafted SWF file, an attacker may be able to execute arbitrary code. Adobe has released Shockwave Player 11.5.1.601 because previous versions used a vulnerable version of the Microsoft Active Template Library (ATL). Additionally, Adobe has released Flash Player 10.0.22.87 and 9.0.246.0 to address the ATL issue and additional vulnerabilities in Flash Player. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code.

Adobe Security Advisory APSA09-03 describes a vulnerability affecting the Adobe Flash player. Flash player version 10.0.22.87 and earlier 10.x versions as well as Flash player version 9.0.159.0 and earlier 9.x versions are affected. An attacker could exploit this vulnerability by convincing a user to visit a website that hosts a specially crafted SWF file. The Adobe Flash browser plugin is available for multiple web browsers and operating systems, any of which could be affected. An attacker could also create a PDF document that has an embedded SWF file to exploit the vulnerability. This vulnerability is being actively exploited.

These vulnerabilities can be mitigated by disabling the Flash plugin or by using the NoScript extension for Mozilla Firefox or SeaMonkey to whitelist websites that can access the Flash plugin. For more information about securely configuring web browsers, please see the Securing Your Web Browser document. US-CERT Vulnerability Note VU#259425 has additional details, as well as information about mitigating the PDF document attack vector.

US-CERT encourages users and administrators to review Adobe security bulletins APSB09-11 and APSB09-10 and apply any necessary updates to help mitigate the risks. Additional information can be found in the Adobe PSIRT blog and in Adobe security advisory APSA09-04. Additional information regarding this vulnerability can be found in US-CERT Technical Cyber Security Alert TA09-204A.

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