US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary

- August 2008 -

This report summarizes general activity as well as updates made to the National Cyber Alert System for the month of August. 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 the month of August 2008, US-CERT issued 16 current activity entries, one (1) technical cyber security alert, one (1) cyber security alert, four (4) weekly cyber security bulletin summary reports, and two (2) cyber security tips.

Highlights for this month include multiple updates released by Apple, Oracle, and Microsoft; a fraudulent Flash Player update; attacks on Linux-based systems using compromised SSH keys, and multiple phishing and spam campaigns.

Contents

Current Activity

Current Activity entries are high-impact types of security incidents currently being reported to US-CERT. This month's highlights and activity are listed below.

- Apple released Security Update 2008-05 to address vulnerabilities in BIND, CoreGraphics, OpenSSL, and other software. Additionally, it addressed weaknesses in common DNS implementations that could allow attackers to execute arbitrary code or perform other malicious activities.
- Oracle released a patch for the WebLogic plug-in for Apache to address a buffer overflow vulnerability that could allow a remote attacker to execute arbitrary code or cause a denial-of-service condition.
- Microsoft's August Security Bulletin addressed multiple vulnerabilities in Microsoft Windows, Office, Internet Explorer, Outlook Express, Windows Mail, and Windows Messenger. Additionally, Microsoft released an updated Security Bulletin that addressed a vulnerability in PowerPoint.
- Internet System Consortium (ISC) released updates for BIND to address performance and stability issues.

- Adobe issued a security bulletin to warn users of malware regarding a fraudulent Flash Player installer. The worm spreads via fraudulent posts on social networking sites, which include links to fake sites that prompt users to update their versions of Flash Player. If users attempt to use the installer to make the update, malware may be downloaded and installed onto their systems.
- Red Hat released a security advisory to address an incident that involved an intrusion on several of their computer systems. During the intrusion, an attacker was able to sign a small number of OpenSSH packages. Red Hat provided a list of the compromised packages and has released updated versions of the OpenSSH packages as a precautionary measure.
- US-CERT became aware of reports regarding attacks on Linux-based systems using compromised SSH keys. More information is provided in the Security Highlights section of this document.

Current Activity for August 2008	
August 1	Apple Releases Security Update 2008-005
August 4	CA ARCserve Backup for Laptops and Desktops Server vulnerability
August 4	Internet System Consortium releases BIND -P2 patches
August 5	Malware Targeting Adobe Flash Player
August 6	Oracle Releases Patch for WebLogic Plug-in Vulnerability
August 7	Microsoft Releases Advanced Notification for August Security Bulletin
August 7	Malware Circulating via Spam Messages
August 12	Microsoft Releases August Security Bulletin
August 13	Apple MobileMe Phishing Scam
August 14	Joomla! Password Reset Vulnerability
August 18	Webex Meeting Manager ActiveX Control Vulnerability
August 21	Malware Circulating via Russia/Georgia Conflict Spam Messages
August 21	Opera Releases Version 9.52
August 25	Microsoft Revised Security Bulletin MS08-051
August 25	Red Hat Releases OpenSSH Security Update
August 27	SSH Key-based Attacks

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 August 2008	
August 12	TA08-225A 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.

Cyber Security Alerts (non-technical) for August 2008	
August 12	SA08-225A Microsoft Updates for Multiple Vulnerabilities

Cyber Security Bulletins

Cyber Security Bulletins are issued weekly and provide a summary of new vulnerabilities that have been 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 August 2008
SB08-217 Vulnerability Summary for the Week of July 28, 2008
SB08-224 Vulnerability Summary for the Week of August 4, 2008
SB08-231 Vulnerability Summary for the Week of August 11, 2008
SB08-238 Vulnerability Summary for the Week of August 18, 2008

A total of 367 vulnerabilities were recorded in the NVD during August 2008.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users and are issued every two weeks. August's tips focused on internationalized domain names and electronic devices. Links to the full versions of these documents are listed below.

Cyber Security Tips for August 2008	
August 6	ST05-016 Understanding Internationalized Domain Names
August 20	ST05-017 Cybersecurity for Electronic Devices

Security Highlights

Compromised SSH Keys Used in Attacks Against Linux-based Systems

US-CERT became aware of active attacks against Linux-based computing infrastructures using compromised SSH keys. The attack appeared to initially use stolen SSH keys to gain access to a system, and then use local kernel exploits to gain root access. Once root access has been obtained, a rootkit known as "phalanx2" is installed.

Phalanx2 appears to be a derivative of an older rootkit named "phalanx". Phalanx2 and the support scripts within the rootkit are configured to systematically steal SSH keys from the compromised system. These SSH keys are sent to the attackers who then use them to try to compromise other sites and systems of interest at the attacked site.

US-CERT released a Current Activity on the public website (www.us-cert.gov) to detail this compromise and provide detection methods and mitigation strategies.

Phishing and Spam Updates

In addition to malware being spread via a fraudulent Flash Player installer, US-CERT received reports of other malware spreading via spam. Malware had been reported spreading via spam messages related to the Olympics and to fake CNN news reports. If users click the link to one of these fake news reports, they are prompted to install a Flash Player update. If users then attempt to install the update, malware may be downloaded and installed onto their system.

Other malware was reported to be circulating via spam email messages related to the Russia/Georgia conflict. These messages contained factual information about the conflict with download instructions for the user to watch a video attached to the message. If users open the attachment, malware may be downloaded and installed onto their system.

Addtionally, phishing attacks circulating via email messages were reported to be targeting Apple MobileMe users. These messages falsely claimed that there was a problem with the user's billing information and instructed the user to click on a link to update personal information. Clicking on this link directs the user to a web page that contains a seemingly legitimate web form requesting personal and financial information. Any information entered in this form is actually sent to a malicious attacker instead of Apple.

US-CERT released a Current Activity entry to detail each of these issues and provide mitigation strategies.

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: 0x7C15DFB9
PGP Key Fingerprint: 673D 044E D62A 630F CDD5 F443 EF31 8090 7C15 DFB9
PGP Key: https://www.us-cert.gov/pgp/info.asc