US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary

- March 2008 -

This report summarizes general activity as well as updates made to the National Cyber Alert System for the month of March. 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 March 2008, US-CERT issued 25 current activity updates, six (6) technical cyber security alerts, four (4) cyber security alerts, four (4) weekly cyber security bulletin summary reports, and two (2) cyber security tips.

Highlights for this month include massive web page infections through SQL and IFRAME injections; security updates from Cisco, Microsoft, and Apple; and email scams involving the Internal Revenue Service.

Contents

Current Activity

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

- Cisco released Security Advisory cisco-sa-20080312-ucp to address multiple vulnerabilities in the Cisco Secure Access Control Server for Windows User-Changeable Password (UCP) application. These vulnerabilities are due to buffer overflow conditions and improper sanitization of input passed to CSuserCGI.exe. Exploitation of these vulnerabilities may allow a remote, unauthenticated attacker to execute arbitrary code.
- Cisco released five security advisories to address multiple vulnerabilities in Cisco IOS. These vulnerabilities may allow a remote, unauthenticated attacker to cause a denial-of-service condition on the affected device.
- Microsoft released security updates to address vulnerabilities in Microsoft Excel, Outlook, Office, and Office Web Components as part of the Microsoft Security Bulletin Summary for March 2008. Microsoft also re-released MS08-014 to include additional information about issues relating to users of Excel 2003 Service Pack 2 or Service Pack 3.
- Apple released Safari 3.1 and Security Update 2008-002 to address multiple vulnerabilities.

Current Activity for March 2008	
March 5	Increased Traffic to 7100/udp
March 6	Sun Java SE Updates
March 6	Microsoft Releases Advance Notification for March Security Bulletin
March 7	GNOME Evolution Vulnerability
March 11	RealPlayer ActiveX Vulnerability
March 11	Microsoft Releases March Security Bulletin
March 11	Trojan Exploiting Microsoft Excel Vulnerability
March 12	Cisco Releases Security Advisory to Address Multiple Vulnerabilities
March 12	Adobe Releases Security Bulletins to Address Multiple Vulnerabilities
March 14	Websites Compromised Through SQL Injection
March 14	Search Engine IFRAME Injection Attacks
March 17	Microsoft Updates March Security Bulletin
March 18	CA BrightStor ARCserve Backup Vulnerability
March 18	F-Secure Releases Security Bulletin
March 19	Microsoft Releases Windows Vista Service Pack 1
March 19	MIT Kerberos Security Advisories
March 19	Apple Security Updates
March 19	VMware Security Advisory
March 21	Microsoft Jet Database Engine Vulnerability
March 21	Apple Aperture and iPhoto Vulnerability
March 26	Mozilla Releases Firefox 2.0.0.13
March 26	Cisco Releases Security Advisories
March 26	Novell eDirectory Vulnerability
March 26	VLC Media Player Vulnerability
March 31	Internal Revenue Service Scams

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 March 2008	
March 6	TA08-066A Sun Updates for Multiple Vulnerabilities in Java
March 11	TA08-071A Microsoft Updates for Multiple Vulnerabilities
March 19	TA08-079A Apple Updates for Multiple Vulnerabilities
March 19	TA08-079B MIT Kerberos Updates for Multiple Vulnerabilities
March 27	TA08-087B Cisco Updates for Multiple Vulnerabilities
March 27	TA08-087A Mozilla 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 computer users can take to protect themselves from attack.

Security Alerts (non-technical) for March 2008	
March 6	SA08-066A Sun Updates for Multiple Vulnerabilities in Java
March 11	SA08-071A Microsoft Updates for Multiple Vulnerabilities
March 19	SA08-079A Apple Updates for Multiple Vulnerabilities
March 27	SA08-087A Mozilla 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 March 2008
SB08-070Vulnerability Summary for the Week of March 3, 2008
SB08-077Vulnerability Summary for the Week of March 10, 2008
SB08-084Vulnerability Summary for the Week of March 17, 2008
SB08-091Vulnerability Summary for the Week of March 24, 2008

A total of 506 vulnerabilities were recorded in the NVD during March 2008.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users and are issued twice a month. March's tips focused on reviewing end-user license agreements, and recovering from viruses, worms, and Trojan horses.

Cyber Security Tips for March 2008	
March 5	ST05-005 Reviewing End-User License Agreements
March 19	ST05-006 Recovering from Viruses, Worms, and Trojan Horses

Security Highlights

- A large number of legitimate web pages were compromised via embedded references to JavaScript code. This code attempts to exploit known vulnerabilities for which patches are available but may not have been applied to the victim's system.
- Other massive website attacks used specially crafted URLs that injected IFRAMEs as terms into search engines on legitimate websites. These infected sites may exploit web browser vulnerabilities, entice users to download and install malicious code, or display unsolicited advertisements.
- A new series of email scams related to the United States Internal Revenue Service (IRS) began to circulate with the approach of the tax filing deadline. The attacks use email to convince users to perform the following actions:
  - Open an email attachment containing bogus tax documents that are embedded with malicious code
  - Follow a link to an unofficial tax website that contains malicious code
  - Follow a link to an unofficial tax website that requests personal information from the users as part of a phishing attack
  - Call an unofficial phone number that requests personal information from the user as part of a phishing attack

  Refer to the Internal Revenue Service Suspicious e-Mails and Identity Theft website for more information on current scams.

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