US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary
- November 2007 -

This report summarizes general activity as well as updates made to the National Cyber Alert System for the month of November. 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 November 2007, US-CERT issued seventeen (17) current activity updates, four (4) technical cyber security alerts, four (4) cyber security alerts, two (2) cyber security tips, and four (4) weekly cyber security bulletin summary reports.

Security highlights this month include the phishing email impersonating government agencies, multiple updates from Apple and Microsoft, the Cyber Security Awareness Summit, and the FBI's Operation Bot Roast II.

Contents

Executive Summary…..……………………….1
Current Activity…….…………..…..……………1
Technical Cyber Security Alerts………..….2
Cyber Security Alerts………………….…….2
Cyber Security Bulletins……………………..3
Cyber Security Tips…………………………..3
Security Highlights……………………………3
Contacting US-CERT…………………………4

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.

- The FBI, along with other participating entities, conducted Operation Bot Roast II. The effort yielded several high profile indictments of botnet operators responsible for as much as US$20 million in economic losses.
- New fraudulent emails purporting to be from the Department of Justice were identified. The Internal Revenue Service and the Federal Trade Commission have previously been targeted by similar scams.
- Apple and Microsoft released multiple patches for their respective operating systems and other software.

Current Activity for November 2007	
November 1	Mac DNS Changer Trojan
November 6	Mac OS X Leopard Firewall Changes
November 7	Apple Releases Security Update to Address Multiple QuickTime Vulnerabilities

Current Activity for November 2007	
November 8	Microsoft Releases Advance Notification for November Security Bulletin
November 8	Microsoft Releases Security Advisory to Address Macrovision Vulnerability
November 9	Public Exploit for Oracle Database Server Vulnerability
November 13	Microsoft Releases November Security Bulletins
November 15	Mac OS X Leopard Firewall Changes
November 15	Apple Releases Security Updates to Address Multiple Vulnerabilities
November 15	False Microsoft Update Emails Circulating
November 19	Trojan Spreading via MSN Messenger
November 20	Department of Justice Fraudulent Spam Email Variant
November 21	iFrame Attack Affects Monster.com
November 27	Vulnerability in Apple QuickTime
November 28	Search Engines Results Linking to Malicious Web Sites
November 29	FBI Announces Results of Operation Bot Roast II
November 29	IBM Lotus Notes Email Attachment Vulnerability

Technical Cyber Security Alerts

Technical Cyber Security Alerts are distributed to provide timely information about current security issues, vulnerabilities, and exploits.

- Apple issued multiple updates for its Mac OS X and Mac OS X Sever Operating Systems. The patch for version 10.4.11 addressed multiple vulnerabilities including those from third party software that ship with the operating systems. The multimedia QuickTime application was also updated to version 7.3.
- Microsoft's November updates addressed vulnerabilities in URI handling and DNS spoofing in its various Windows Operating Systems.

Technical Cyber Security Alerts for November 2007	
November 6	TA07-310A Apple QuickTime Updates for Multiple Vulnerabilities
November 13	TA07-317A Microsoft Updates for Multiple Vulnerabilities
November 15	TA07-319A Apple Updates for Multiple Vulnerabilities
November 30	TA07-334A Apple QuickTime RTSP Buffer Overflow

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 November 2007	
November 6	SA07-310A Apple QuickTime Updates for Multiple Vulnerabilities
November 13	SA07-317A Microsoft Updates for Multiple Vulnerabilities
November 15	SA07-319A Apple Updates for Multiple Vulnerabilities
November 30	SA07-334A Apple QuickTime RTSP Vulnerability

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 November 2007
Vulnerability Summary for the Week of November 5, 2007
Vulnerability Summary for the Week of November 12, 2007
Vulnerability Summary for the Week of November 19, 2007
Vulnerability Summary for the Week of November 26, 2007

A total of 424 vulnerabilities were recorded in the NVD during November 2007.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users and are issued twice a month. November's tips focused on understanding web browsers and email clients. Links to the full versions of these documents are listed below.

Cyber Security Tips for November 2007	
November 15	ST04-022 Understanding Your Computer: Web Browsers
November 23	ST04-023 Understanding Your Computer: Email Clients

Security Highlights

DHS Cyber Security Awareness

The Department of Homeland Security (DHS) kicked off Cyber Security Awareness Month in October with the National Cyber Security Awareness Summit. Held in Washington, DC, this event included industry leaders and partnership organizations to focus on educating the American public, businesses, schools and government agencies about securing their portion of cyber space and the nation's critical infrastructures.

The DHS Assistant Secretary of Cyber Security and Communications, Greg Garcia, discussed the Department's collaborative efforts with various organizations to protect against cyber security threats. Along with other remarks, the Assistant Secretary outlined three priorities:

> 1) Secure federal systems: To secure federal systems, the department is expanding participation from other agencies into the Einstein program. As a whole, the Einstein program provides a big picture view of network activity occurring on federal computer systems.
>
> 2) Build a comprehensive risk management framework: The National Infrastructure Protection Plan (NIPP) forms the underlying foundation for a risk management framework.
>
> 3) Enhance cyber response operational capabilities: Part of US-CERT's mission is to improve situational awareness among constituents by increasing analytical capabilities and coordinating response to cyber incidents. This improves operational capabilities by enabling organizations to see potential trends and develop appropriate prevention and response measures.

As threats continue to be pervasive, it becomes more critical for individual users and organizations to share these priorities and increase awareness of cyber security practices to the public at large. The entirety of the Assistant Secretary's remarks can be found at: http://www.dhs.gov/xnews/releases/pr_1191270671928.shtm. For more information regarding cyber security, or to sign-up to receive security updates and tips, visit http://www.us-cert.gov/cas/signup.html.

Operation Bot Roast II

On November 29, 2007, the FBI announced the results of the second phase of its continuing investigation into the criminal use of botnets. Since Operation 'Bot Roast' was announced last June, eight individuals have been indicted, pled guilty, or been sentenced for crimes related to botnet activity. Additionally, thirteen search warrants were served in the U.S. and by overseas law enforcement partners in connection with this operation. It is anticipated that more than $20 million in economic loss and over one million victim computers will be uncovered during Operation Bot Roast II.

US-CERT works closely with the FBI to investigate and identify cyber criminals and threats. US-CERT and the FBI will continue to monitor this activity and provide updates as needed. To view the press release in full, visit http://www.fbi.gov/page2/nov07/botnet112907.html.

Contacting US-CERT

If you would like to contact US-CERT to ask a question or submit an incident, 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