US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary
- November 2011 -

This report summarizes general activity including updates to the National Cyber Alert System in November 2011. It includes current activity updates, technical and non-technical cyber security alerts, and cyber security bulletins, in addition to other newsworthy events or highlights.

Executive Summary

During November 2011, US-CERT issued 13 Current Activity entries, a Technical Cyber Security Alert, a Cyber Security Alert, and four weekly Cyber Security Bulletins.

Highlights for this month include updates or advisories released by Microsoft, Apple, Google, Adobe, and The Mozilla Foundation.

Contents

Current Activity

Current Activity entries are high-impact security threats and vulnerabilities currently reported to US-CERT. The table lists all of the entries posted this month followed by a brief overview of the most significant entries.

Current Activity for November 2011	
November 3	Microsoft Releases Advance Notification for November Security Bulletin
November 4	Microsoft Releases Security Advisory for Vulnerability in TrueType Font Parsing
November 8	Microsoft Releases November Security Bulletin
November 8	Adobe Releases Security Bulletin for Adobe Shockwave Player
November 9	Mozilla Releases Firefox 8 and 3.6.24
November 10	Operation Ghost Click Malware
November 10	Google Releases Chrome 15.0.874.120
November 10	Apple Releases iOS 5.0.1
November 10	Fraudulent Digital Certificates Could Allow Spoofing
November 11	Adobe Releases Security Advisory for Adobe Flash Player and Adobe AIR
November 15	Apple Releases iTunes 10.5.1
November 17	Internet Systems Consortium Releases BIND-P1 Patches
November 17	Google Releases Chrome 15.0.874.121

- Microsoft released updates to address vulnerabilities in Microsoft Windows as part of the Microsoft Security Bulletin Summary for November 2011. These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, or operate with elevated privileges. US-CERT encourages users and administrators to review the bulletin and follow best-practice security policies to determine which updates should be applied.
- Apple released two security updates during the month of November 2011:
    - iTunes 10.5.1 addressed a vulnerability that may allow an attacker to conduct a man-in-the-middle attack that could lead a user to click on a forged link believed to have originated from Apple.
    - iOS 5.0.1 for the iPhone 3GS, iPhone 4, iPhone 4S, iPod 3rd generation or later, iPad, and iPad 2 addressed multiple vulnerabilities that may allow an attacker to execute arbitrary code or obtain sensitive information.
- Google released two updates to its Chrome web browser, Chrome 15.0.874.120 and Chrome 15.0.874.121 for Linux, Mac, Windows, and Chrome Frame, to address multiple vulnerabilities that may allow an attacker to execute arbitrary code.
- Adobe released two Security Bulletins in November 2011:
    - Adobe Security Bulletin APSB11-27 addressed multiple vulnerabilities affecting Shockwave Player 11.6.1.629 and earlier versions for the Windows and Macintosh operating systems. Successful exploitation of these vulnerabilities may allow an attacker to execute arbitrary code.
    - Adobe Security Bulletin APSB11-28 addressed vulnerabilities affecting Adobe Flash Player 11.0.1.152 and earlier versions for Windows, Macintosh, Linux, Solaris, Adobe Flash Player 11.0.1.153 for Android, and Adobe AIR 3.0 for Windows, Macintosh, and Android. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition.
- The Mozilla Foundation released Firefox 8 and Firefox 3.6.24 to address multiple vulnerabilities that may allow an attacker to execute arbitrary code, operate with escalated privileges, cause a denial-of-services condition, obtain sensitive information, or perform a cross-site scripting attack.

Technical Cyber Security Alerts

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

Technical Cyber Security Alerts for November 2011	
November 8	TA11-312A Microsoft Updates for Multiple Vulnerabilities

Cyber Security Alerts

Cyber Security Alerts 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 November 2011	
November 8	SA11-312A Microsoft Updates for Multiple 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's (NIST's) National Vulnerability Database (NVD). The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD)/US-CERT. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

Cyber Security Bulletins for November 2011	
November 7	SB11-311 Vulnerability Summary for the Week of October 31, 2011
November 14	SB11-318 Vulnerability Summary for the Week of November 7, 2011
November 21	SB11-325 Vulnerability Summary for the Week of November 14, 2011
November 28	SB11-332 Vulnerability Summary for the Week of November 21, 2011

A total of 309 vulnerabilities were recorded in the NVD during November 2011.

Security Highlights

Microsoft Releases Security Advisory for Vulnerability in TrueType Font Parsing

Microsoft released Microsoft Security Advisory 2639658 to address a vulnerability in the Win32k TrueType font parsing engine. By convincing a user to open a malicious email attachment, an attacker may be able to exploit this vulnerability and execute arbitrary code.

Microsoft has indicated that it is aware of targeted attacks exploiting this vulnerability. The Duqu malware may exploit this vulnerability.

US-CERT encourages users and administrators to take the following actions to help mitigate the risks of this vulnerability and the Duqu malware:

- Review Microsoft Security Advisory 2639658 and apply the security update in Microsoft Security Bulletin MS11-087.
- Use caution when opening attachments in email messages.
- Maintain up-to-date antivirus software.

FBI Announces Operation Ghost Click

On November 9, 2011, US Federal prosecutors announced Operation Ghost Click, an ongoing investigation that resulted in the arrests of a cyber ring of seven people who allegedly ran a massive online advertising fraud scheme that used malicious software to infect at least 4 million computers in more than 100 countries.

The cyber ring, composed of individuals from Estonia and Russia, allegedly used the malicious software, or malware, to hijack web searches to generate advertising and sales revenue by diverting users from legitimate websites to websites run by the cyber ring. In some cases, the software, known as DNSChanger, would replace advertising on popular websites with other ads when viewed from an infected computer. The malware also could have prevented users' antivirus software from functioning properly, thus exposing infected machines to unrelated malicious software.

US-CERT encourages users and administrators to use caution when surfing the web and to take the following preventative measures to protect themselves from malware campaigns:

- Refer to the FBI's announcement of Operation Ghost Click for additional information on how to protect yourself and recover from DNSChanger attacks.
- Maintain up-to-date antivirus software.
- Configure your web browser as described in the Securing Your Web Browser document.
- Do not follow unsolicited web links in email messages.
- Use caution when opening email attachments. Refer to the Using Caution with Email Attachments Cyber Security Tip for more information on safely handling email attachments.

Contacting US-CERT

If you would like to contact US-CERT to ask a question, submit an incident, or 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
E-mail Address: info@us-cert.gov
Phone Number: +1 (888) 282-0870
PGP Key ID: 0xEDA10949
PGP Key Fingerprint: 6040 50FC 1BA3 81FA 0919 1378 C036 EDA1 0949
PGP Key: https://www.us-cert.gov/pgp/info.asc