US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary
- November 2010 -

This report summarizes general activity as well as updates made to the National Cyber Alert System in November 2010. It 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 November 2010, US-CERT issued ten Current Activity entries, one Technical Cyber Security Alert, one Cyber Security Alert, five weekly Cyber Security Bulletins, and one Cyber Security Tip.

Highlights for this month include updates or advisories released by Adobe, Apple, Microsoft, and OpenSSL; fraud advisories for holiday season consumers; and security practices when using removable media.

Contents

Current Activity

Current Activity entries are high-impact security threats and vulnerabilities presently being 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 2010	
November 1	Removable Media Security Practices
November 9	Microsoft Releases November Security Bulletin
November 9	Insecure Loading of Dynamic Link Libraries in Windows Applications
November 10	Adobe Releases Security Update for Flash Media Server
November 16	Apple Releases Mac OS X v10.6.5 and Security Update 2010-007
November 16	Adobe Releases Security Updates for Reader and Acrobat
November 17	OpenSSL Releases OpenSSL 1.0.0b
November 18	Holiday Season Phishing Scams and Malware Campaigns
November 19	Apple Releases Safari 5.0.3 and 4.1.3
November 23	Apple Releases iOS 4.2

- Adobe addressed multiple vulnerabilities in Acrobat, Reader, and Flash Media Server:
  - Security Advisory APSB10-27 addressed critical vulnerabilities affecting Adobe Flash Media Server (FMS) 4.0 and earlier versions, Adobe Flash Media Server (FMS) 3.5.3 and earlier versions, and Adobe Flash Media Server (FMS) 3.0.6 and earlier versions for Windows and Linux. One of the vulnerabilities could have allowed an attacker, who successfully exploited the vulnerability, to run malicious code on the affected system.
  - Security Advisory APSB10-28 alerted users of critical vulnerabilities identified in Adobe Reader 9.4 (and earlier versions) for Windows, Macintosh and UNIX, and Adobe Acrobat 9.4 (and earlier 9.x versions) for Windows and Macintosh. These vulnerabilities could cause the application to crash and potentially allow an attacker to take control of the affected system.
- Microsoft released two Security Bulletins:
  - Microsoft Security Bulletin Summary for November 2010 addressed vulnerabilities in Microsoft Office and Microsoft Remote Access Software. These vulnerabilities allowed an attacker to execute arbitrary code or operate with elevated privileges.
  - Microsoft Security Bulletin MS10-087 for Microsoft Office addressed one publicly disclosed critical vulnerability related to how some Windows applications loaded external dynamic link libraries (DLLs) that allowed remote code execution if a user opened or viewed a specially crafted Rich Text Format (RTF) document. This security update also addressed five privately reported Microsoft Office vulnerabilities.
- OpenSSL released OpenSSL 1.0.0b, which addressed a vulnerability that allowed an attacker to execute arbitrary code. Any OpenSSL-based TLS server was vulnerable if it was multi-threaded and used OpenSSL's internal caching mechanism. Servers that were multi-process or disabled internal session caching were not affected.
- Apple released updates for Mac OS X, Safari web browser, and iOS to address multiple vulnerabilities.
  - Mac OS X v10.6.5, Mac OS X Server v10.6.5 (10H575), and Security Update 2010-007 addressed multiple vulnerabilities that affected a number of packages. Exploitation of these vulnerabilities would have allowed an attacker to execute arbitrary code, obtain sensitive information, conduct cross-site scripting attacks, cause a denial-of-service condition, or bypass security restrictions. Details can be found in Apple articles HT4435 and HT4452.
  - Safari 5.0.3 and 4.1.3 addressed multiple vulnerabilities in the Safari and WebKit packages. These vulnerabilities allowed an attacker to execute arbitrary code or cause a denial-of-service condition. More information can be found in Apple article HT4455.
  - iOS 4.2 for the iPhone, iPod Touch, and iPad addressed multiple vulnerabilities. Exploitation of these vulnerabilities allowed an attacker to execute arbitrary code, initiate a call, cause a denial-of-service condition, gain system privileges, or obtain sensitive information. More information is provided in Apple article HT4456.
- US-CERT posted information on the possibility of holiday season phishing scams and malware campaigns. Examples of past scams and campaigns, as well as preventative measures, were also provided.

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 November 2010	
November 9	TA10-313A 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 November 2010	
November 9	SA10-313A 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.

Security Bulletins for November 2010
SB10-305 Vulnerability Summary for the Week of October 25, 2010
SB10-312 Vulnerability Summary for the Week of November 1, 2010
SB10-319 Vulnerability Summary for the Week of November 8, 2010
SB10-326 Vulnerability Summary for the Week of November 15, 2010
SB10-333 Vulnerability Summary for the Week of November 22, 2010

A total of 278 vulnerabilities were recorded in the NVD during November 2010.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users. The November tip focused on understanding Voice over Internet Protocol (VoIP).

Cyber Security Tips for November 2010	
November 15	ST05-018 Understanding Voice over Internet Protocol (VoIP)

Security Highlights

Holiday Season Phishing Scams and Malware Campaigns

In the past, US-CERT has received reports of an increased number of phishing scams and malware campaigns that take advantage of the winter holiday and holiday shopping season. US-CERT reminds users to remain cautious when receiving unsolicited email messages that could be part of a potential phishing scam or malware campaign.

These phishing scams and malware campaigns may include but are not limited to the following:

- Electronic greeting cards that may contain malware.
- Requests for charitable contributions that may be phishing scams and may originate from illegitimate sources claiming to be charities.
- Screensavers or other forms of media that may contain malware.
- Credit card applications that may be phishing scams or identity theft attempts.
- Online shopping advertisements that may be phishing scams or identity theft attempts from bogus retailers.

US-CERT encourages users and administrators to use caution when encountering these types of email messages and refer to *Cyber Security Tip ST04-014 "Avoiding Social Engineering and Phishing Attacks"* and *Cyber Security Tip ST07-001 "Shopping Safely Online"* for more information.

Microsoft Insecure Loading of Dynamic Link Libraries in Windows Applications

US-CERT is aware of a class of vulnerabilities, first reported August 25, 2010, related to how some Windows applications may load external dynamic link libraries (DLLs). When an application loads a DLL without specifying a fully qualified path name, Windows will attempt to locate the DLL by searching a defined set of directories. If an application does not securely load DLL files, an attacker may be able to cause the affected application to load an arbitrary library.

Numerous third parties have issued updates to their own programs to help mitigate the risks in the past months. Microsoft released updates for multiple Microsoft Office versions on November 9, 2010 to help mitigate the risk of exploitation of this vulnerability by modifying the way that Microsoft Office software parses files and ensuring a vulnerable component of Microsoft Office uses a more appropriate and secure search order when loading libraries.

Please be aware that although particular software programs have been updated against this vulnerability, the vulnerability still remains in the Windows operating system itself.

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 e-mail 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: 0x91D70D64
PGP Key Fingerprint: EAAC 46A4 4CEC 8A78 EED2 73F3 E5F3 5D6C 91D7 0D64
PGP Key: https://www.us-cert.gov/pgp/info.asc