US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary
- December 2008 -

This report summarizes general activity as well as updates made to the National Cyber Alert System for the month of December. 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 December 2008, US-CERT issued 26 Current Activity entries, four (4) Technical Cyber Security Alerts, four (4) Cyber Security Alerts, five (5) weekly Cyber Security Bulletins, and one (1) Cyber Security Tip.

Highlights for this month included multiple advisories released by Microsoft (MS); updates by Sun, Apple, Mozilla, and Opera; phishing scams regarding airline tickets and electronic greeting cards; weaknesses in certificate signatures using MD5; and an Internet Explorer data binding vulnerability.

Contents

Current Activity

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

- Microsoft issued a security bulletin and multiple security advisories:
  - Microsoft released its December Security Bulletin, which included updates for Windows Media Player, Word, Excel, and Internet Explorer.
  - Microsoft Security Advisory 960906 provided a workaround for a vulnerability in WordPad.
  - Security Bulletin MS08-078 addressed the Internet Explorer vulnerabilities described in Security Advisories 961051 and 960714. A public report also warned of a worm in circulation with the capability of exploiting the patched vulnerability described in Security Bulletin MS08-067.
  - Security Advisory 961040 provided a workaround for a vulnerability in Microsoft SQL Server.
- Apple released security updates to address vulnerabilities in multiple components of Mac OS X and the Adobe Flash Player plug-in.

- Sun released updates to address multiple security issues in Java Runtime Environment (JRE) and Java SE Development Kit (JDK).
- Opera released version 9.63 of its web browser to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code, conduct cross-site scripting attacks, or cause a denial-of-service condition.
- Mozilla released Firefox version 3.0.5 and Thunderbird 2.0.0.19 to address multiple vulnerabilities, some of which are common across both applications. The Firefox vulnerabilities included cross-site scripting and information disclosure. The Thunderbird vulnerabilities included arbitrary code execution, information disclosure, and denial of service.
- Several public reports identified malware spreading through social networking sites and email scams. Messages sent via social networking sites attempted to lure users with a link to a video, which then requests the users to download malware disguised as a fraudulent Adobe Flash Player update. Other spam email claimed to be sent from legitimate airlines, which actually contained a malicious attachment disguised as an invoice or airline ticket. The winter holiday theme was also used to entice users into downloading a malicious file disguised as an electronic greeting card.

Current Activity for December 2008	
December 3	Sun Releases Updates for Java SE
December 5	Microsoft Releases Advanced Notification for December Security Bulletin
December 8	Malware Spreading via Social Networking Sites
December 9	Microsoft Releases Security Advisory (960906)
December 9	Microsoft Releases December Security Bulletin
December 9	PHP 5.2.8 Released
December 11	Airline Ticket Email Scam
December 11	CA ARCserve Backup Vulnerability
December 12	Microsoft Releases Security Advisory (961051)
December 15	Apple Releases Security Updates for Multiple Vulnerabilities
December 16	Microsoft Releases Advance Notification
December 17	Microsoft Releases Security Bulletin MS08-078
December 17	Mozilla has released Firefox 3.0.5
December 17	Opera Software releases Opera Version 9.63
December 23	Trend Micro Releases Updates for HouseCall
December 23	Microsoft Releases Security Advisory (961040)
December 31	Rogue MD5 SSL Certificate Vulnerability
December 31	Worm Exploiting Microsoft MS08-067 Circulating
December 31	Mozilla Releases Thunderbird 2.0.0.19
December 31	Malware Spreading via Malicious Ecard

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 December 2008	
December 5	TA08-340A Sun Java Updates for Multiple Vulnerabilities
December 9	TA08-344A Microsoft Updates for Multiple Vulnerabilities
December 15	TA08-350A Apple Updates for Multiple Vulnerabilities
December 17	TA08-352A Microsoft Internet Explorer Data Binding Vulnerability

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 December 2008	
December 5	SA08-340A Sun Java Updates for Multiple Vulnerabilities
December 9	SA08-344A Microsoft Updates for Multiple Vulnerabilities
December 15	SA08-350A Apple Updates for Multiple Vulnerabilities
December 17	SA08-352A Microsoft Internet Explorer Data Binding 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 December 2008
SB08-336 Vulnerability Summary for the Week of November 24, 2008
SB08-343 Vulnerability Summary for the Week of December 1, 2008
SB08-350 Vulnerability Summary for the Week of December 8, 2008
SB08-357 Vulnerability Summary for the Week of December 15, 2008
SB08-364 Vulnerability Summary for the Week of December 22, 2008

A total of 529 vulnerabilities were recorded in the NVD during December 2008.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users and are issued every two weeks. December's tips focused on shopping safely online.

Cyber Security Tips for December 2008	
December 3	ST07-001 Shopping Safely Online

Security Highlights

Vulnerability in Certificates Using MD5 Signatures
US-CERT is aware of a public report describing how MD5 collisions can be leveraged to generate rogue SSL CA certificates. A valid certificate implies a level of trust that a specific website is legitimate. With this vulnerability, however, a rogue CA certificate could be used by an attacker to generate valid SSL certificates for arbitrary websites. Using these certificates in DNS redirection attacks, an attacker could spoof an SSL-protected website and obtain sensitive information by misleading a user into supplying sensitive information.

As stated in US-CERT Vulnerability Note VU#836068, most operating systems bundle a collection of trusted CA certificates, including some that use the MD5 signing algorithm, providing obvious targets for attackers to spoof. This can be used to mislead a user into supplying sensitive information to a malicious website, considering the website appears to be authentic based on the apparently valid signed SSL certificate.

Microsoft Internet Explorer Data Binding Vulnerability
As described in the Technical Cyber Security Alert TA08-352A, Microsoft Internet Explorer (IE) contains an invalid pointer vulnerability in its data binding code. Specially crafted content that performs data binding, such as XML or HTML documents, can cause IE to crash in a way that is exploitable. Limited testing has shown this vulnerability to affect Internet Explorer versions 6 through 8 Beta 2, although all versions from 4.0 and later may be at risk. Outlook Express is also at risk.

The vulnerability can be triggered when Internet Explorer or a program that uses Internet Explorer's components renders a document that contains more than one reference to the same data source. This flaw can cause an invalid array size and result in the accessing of memory space of a deleted object. Exploit code for this vulnerability is publicly available. By convincing a user to view a specially crafted document that performs data binding (e.g., a web page or email message or attachment), an attacker may be able to execute arbitrary code with the privileges of the user.

This issue is addressed in Microsoft Security Bulletin MS08-078. This update provides new versions of `mshtml.dll` and `wmshtml.dll`, depending on the target operating system. More details are available in Microsoft Knowledge Base Article 960714.

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: CF5B48C2
PGP Key Fingerprint: 01F1 9C58 0817 D612 45ED 3FCF 3004 FE8C CF5B 48C2 PGP Key: https://www.us-cert.gov/pgp/info.asc