US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary
- September 2011 -

This report summarizes general activity including updates to the National Cyber Alert System in September 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 September 2011, US-CERT issued 12 Current Activity entries, one Technical Cyber Security Alert, one Cyber Security Alert, and four weekly Cyber Security Bulletins.

Highlights for this month include updates or advisories released by Microsoft, Adobe, Google, and Cisco. Also notable were public reports of fraudulent SSL certificates issued by DigiNotar and of a vulnerability affecting the SSL and TLS protocols.

Contents

Executive Summary……1

Current Activity……1

Technical Cyber Security Alerts……2

Cyber Security Alerts……3

Cyber Security Bulletins……3

Security Highlights……3

Contacting US-CERT……3

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 September 2011	
September 8	Microsoft Releases Advance Notification for September Security Bulletin
September 9	Adobe Prenotification Security Advisory for Adobe Reader and Acrobat
September 9	Fraudulent DigiNotar SSL Certificate
September 13	Microsoft Releases September Security Bulletin
September 13	Adobe Releases Security Advisory for Adobe Reader and Acrobat
September 14	Cisco Releases Multiple Security Advisories
September 19	Google Releases Chrome 14.0.835.163
September 19	Oracle Releases Security Alert for Oracle HTTP Server Products
September 21	Cisco Releases Security Advisory for Identity Services Engine
September 22	Adobe Prenotification Security Advisory for Adobe Flash Player
September 27	SSL/TLS Protocol Vulnerability

Current Activity for September 2011	
September 29	Cisco Releases Security Advisory for Cisco IOS Software Smart Install

- The Microsoft Security Bulletin Summary for September 2011 provided updates addressing vulnerabilities in Microsoft Windows, Microsoft Office, and Microsoft Server Software. These vulnerabilities may allow an attacker to execute arbitrary code or operate with elevated privileges.
- Adobe released Security Bulletins addressing critical and important vulnerabilities in the following products.
  - Adobe Security Bulletin APSB11-24 addressed multiple vulnerabilities in Adobe Acrobat and Adobe Reader. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code or operate with escalated privileges.
  - APSB11-26 addressed multiple vulnerabilities in Adobe Flash that could potentially allow an attacker to take control of the affected system. One of the vulnerabilities addressed, CVE-2011-2444, is a cross-site scripting (XSS) vulnerability that was exploited in the wild in active targeted email attacks designed to trick the user into clicking on a malicious link.
- Google released Chrome 14.0.835.163 for Linux, Mac, Windows, and Chrome Frame to address multiple vulnerabilities that may allow an attacker to execute arbitrary code.
- Cisco released four security advisories in September 2011 addressing vulnerabilities in multiple products.
  - Advisory cisco-sa-20110914-lms addressed two vulnerabilities in CiscoWorks LAN Management Solution software that could allow an unauthenticated remote attacker to execute arbitrary code on affected servers.
  - cisco-sa-20110914-cusm addressed two vulnerabilities in Cisco Unified Service Monitor and Cisco Unified Operations Manager software that could allow an unauthenticated remote attacker to execute arbitrary code on affected servers.
  - cisco-sa-20110920-ise addressed a vulnerability in Cisco Identity Services Engine that may allow a remote attacker to gain complete administrative control of the device.
  - cisco-sa-20110928-smart-install addressed a vulnerability in the Cisco IOS Software Install feature running on Cisco Catalyst Switches that may allow remote code execution by an unauthenticated attacker.
- US-CERT is aware of a vulnerability affecting the Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols. Exploitation of this vulnerability may allow an attacker to decrypt encrypted SSL/TLS traffic and obtain sensitive information. Microsoft released Security Advisory 2588513 to provide workarounds for this vulnerability in the Windows implementation of the SSL and TLS protocols. Because the SSL and TLS protocols are used in a variety of products, users and administrators are encouraged to check with their software vendors for updated versions. Additional information can be found in Vulnerability Note VU#864643.

Technical Cyber Security Alerts

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

Technical Cyber Security Alerts for September 2011	
September 13	TA11-256A 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 September 2011	
September 13	SA11-256A 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 September 2011	
September 6	SB11-248 Vulnerability Summary for the Week of August 29, 2011
September 13	SB11-255 Vulnerability Summary for the Week of September 5, 2011
September 19	SB11-262 Vulnerability Summary for the Week of September 12, 2011
September 28	SB11-269 Vulnerability Summary for the Week of September 19, 2011

A total of 387 vulnerabilities were recorded in the NVD during September 2011.

Security Highlights

Fraudulent DigiNotar SSL Certificates

US-CERT is aware of public reports of the existence of fraudulent SSL certificates issued by the certificate authority (CA) DigiNotar. An attacker could use these fraudulent SSL certificates to masquerade as legitimate websites. Mozilla, Microsoft, Google, Apple, and Adobe released security updates and removed DigiNotar root certificates from their products' certificate trust lists. US-CERT encourages users and administrators to apply any necessary updates to help mitigate the risks.

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.

Website Address: http://www.us-cert.gov
Email 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