



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary - August 2011 -

This report summarizes general activity including updates to the [National Cyber Alert System](#) in August 2011. 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 August 2011, US-CERT issued 12 Current Activity entries, two Technical Cyber Security Alerts, two Cyber Security Alerts, five weekly Cyber Security Bulletins, and one Cyber Security Tip.

Highlights for this month include updates or advisories released by Microsoft, Adobe, and RIM. Also of note were a paper on Small Office/Home Office Router Security and reports of fraudulent SSL certificates issued after certificate authority DigiNotar was compromised.

Contents

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

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 August 2011	
August 3	Google Releases Chrome 13.0.782.107
August 3	WordPress Themes Vulnerability
August 4	Microsoft Releases Advance Notification for August Security Bulletin
August 4	Apple Releases QuickTime 7.7
August 9	Microsoft Releases August Security Bulletin
August 10	Adobe Releases Security Bulletins for Multiple Products
August 10	RIM Releases Security Advisory for BlackBerry Enterprise Server
August 17	Mozilla Releases Firefox 6 and 3.6.20
August 23	Google Releases Chrome 13.0.782.215
August 25	Cisco Releases Security Advisories

Current Activity for August 2011	
August 29	Potential Hurricane Irene Phishing Scams
August 30	Fraudulent DigiNotar SSL Certificate

- The [Microsoft Security Bulletin Summary for August 2011](#) provided updates to address vulnerabilities in Microsoft Windows, Internet Explorer, Microsoft Office, Microsoft .NET Framework, and Microsoft Developer Tools. These vulnerabilities may allow an attacker to execute arbitrary code, operate with elevated privileges, cause a denial-of-service condition, or disclose sensitive information.
- Adobe released [Security Bulletins](#) to address critical and important vulnerabilities in the following products.
 - Adobe Shockwave Player 11.6.0.626 and earlier versions on the Windows and Macintosh operating systems
 - Adobe Flash Player 10.3.181.36 and earlier versions for Windows, Macintosh, Linux, and Solaris
 - Adobe Flash Player 10.3.185.25 and earlier versions for Android
 - Adobe Flash Media Server 4.0.2 and earlier versions
 - Adobe Flash Media Server 3.5.6 and earlier versions for Windows and Linux
 - Adobe Photoshop CS5 and CS5.1 and earlier for Windows and Macintosh
 - RoboHelp 9.0.1.233 and earlier, RoboHelp 8, RoboHelp Server 9, and RoboHelp Server 8

Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, take control of an affected system, or perform a cross-site scripting attack.

- Research In Motion Limited (RIM) released a security advisory addressing a vulnerability in the BlackBerry MDS Connection Service and BlackBerry Messaging Agent for the BlackBerry Enterprise Server. This vulnerability may allow an attacker to execute arbitrary code or gain unauthorized access to the BlackBerry Enterprise Server.
- US-CERT created a Current Activity entry based on public reports of the existence of at least one fraudulent SSL certificate issued by DigiNotar. This fraudulent SSL certificate could be used by an attacker to masquerade a maliciously designed website as any subdomain of google.com. Based on this information, [Mozilla](#) released new versions of Firefox for desktop (3.6.21, 6.0.1, 7, 8, and 9) and mobile (6.0.1, 7, 8, and 9) and [Microsoft](#) removed the DigiNotar root certificate from the Microsoft Certificate Trust List for all versions of Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2. Microsoft also released an update for Windows XP and Windows Server 2003 to address this issue. [Google](#) decided to reject all the Certificate Authorities operated by DigiNotar. All Google Chrome users are protected from this attack due to Chrome's built-in certificate pinning feature.

Technical Cyber Security Alerts

[Technical Cyber Security Alerts](#) provide timely information about current security issues, vulnerabilities, and exploits.

Technical Cyber Security Alerts for August 2011	
August 9	TA11-221A Microsoft Updates for Multiple Vulnerabilities
August 10	TA11-222A Adobe 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.

<i>Cyber Security Alerts (non-technical) for August 2011</i>	
August 9	SA11-221A Microsoft Updates for Multiple Vulnerabilities
August 10	SA11-222A Adobe 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 (NCSA)/US-CERT. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

<i>Cyber Security Bulletins for August 2011</i>	
August 2	SB11-213 Vulnerability Summary for the Week of July 25, 2011
August 8	SB11-220 Vulnerability Summary for the Week of August 1, 2011
August 16	SB11-227 Vulnerability Summary for the Week of August 8, 2011
August 23	SB11-234 Vulnerability Summary for the Week of August 15, 2011
August 30	SB11-241 Vulnerability Summary for the Week of August 22, 2011

A total of 294 vulnerabilities were recorded in the NVD during August 2011.

Cyber Security Tips

[Cyber Security Tips](#) are primarily intended for non-technical computer users. The focus of August's tip was Internet Service Providers (ISPs).

<i>Cyber Security Tips for August 2011</i>	
August 24	ST06-001 Understanding Hidden Threats: Rootkits and Botnets

Security Highlights

Paper on Small Office/Home Office Router Security

On August 11, 2011, US-CERT released a [paper](#) on small office and home office router security. This paper provides information on how to increase the security of home routers and reduce the vulnerability of the internal network against attacks from external sources.

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>