US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary

- September 2012 -

This report summarizes general activity including updates to the National Cyber Awareness System in September 2012. It includes current activity updates, alerts, and bulletins in addition to other newsworthy events or highlights.

Executive Summary

During September 2012, US-CERT issued five Current Activity entries, four Alerts, and four weekly Bulletins.

Highlights for this month include updates or advisories released by Microsoft and Adobe.

Contents

Current Activity

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

Current Activity for September 2012	
September 6	Microsoft Releases Advance Notification for September Security Bulletin
September 11	Microsoft Releases September Security Bulletin
September 19	Microsoft Releases Security Advisory for Internet Explorer
September 21	Increased Exploitation in Web Content Management Systems
September 28	Adobe Releases Security Bulletin About Code Signing Certificate

- Microsoft released updates to address vulnerabilities in Microsoft Development Tools and Server Software as part of the Microsoft Security Bulletin Summary for September 2012. These vulnerabilities may allow an attacker to 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.
- Microsoft also released Security Advisory 2757760 to address a vulnerability in Microsoft Internet Explorer 6, 7, 8, and 9. This vulnerability may allow an attacker to execute arbitrary code if a user accesses specially crafted HTML documents (e.g., a web page or an HTML email message or attachment). US-CERT encourages users and administrators to review Microsoft

Security Advisory 2757760. This advisory indicates that the workaround does not correct the vulnerability, but it may help mitigate the risk against known attack vectors. Additional information regarding CVE-2012-4969 can be found in US-CERT Technical Alert TA12-262A and Vulnerability Note VU#480095.

- Adobe released a security bulletin to address an issue with an Adobe code signing certificate. The revoked certificate has been used to sign malicious code. The certificate was revoked on October 4, 2012 for all software code signed after July 10, 2012. Adobe issued a new digital certificate for all affected products. US-CERT encourages users and administrators to review the Adobe Security Bulletin APSA12-01 and take any necessary actions to help mitigate the risk.

Alerts

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

Alerts for September 2012	
September 7	TA12-251A Microsoft Update For Minimum Certificate Key Length
September 11	TA12-255A Microsoft Updates for Multiple Vulnerabilities
September 18	TA12-262A Microsoft Security Advisory for Internet Explorer Exploit
September 21	TA12-265A Microsoft Releases Patch for Internet Explorer Exploit

Bulletins

Bulletins are issued weekly and provide a summary of new vulnerabilities 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)/US-CERT. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

Bulletins for September 2012	
September 4	SB12-248 Vulnerability Summary for the Week of August 27, 2012
September 10	SB12-254 Vulnerability Summary for the Week of September 3, 2012
September 17	SB12-261 Vulnerability Summary for the Week of September 10, 2012
September 26	SB12-269 Vulnerability Summary for the Week of September 17, 2012

A total of 655 vulnerabilities were recorded in the NVD during September 2012.

Security Highlights

Increased Exploitation in Web Content Management Systems

US-CERT is aware of recent increases in the exploitation of known vulnerabilities in web content management systems (CMSs) such as Wordpress and Joomla. Compromised CMS installations can be used to host malicious content. US-CERT recommends that users and administrators ensure that their CMS installations are patched or upgraded to remove known vulnerabilities. This may require contacting the hosting provider. Also, users and administrators can check for known vulnerabilities in the National Vulnerability Database by searching their CMS by name.

Contacting US-CERT

If you would like to contact US-CERT to ask a question, submit an incident, or learn more about cybersecurity, 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: soc@us-cert.gov
Phone Number: +1 888-282-0870
PGP/GPG Key: E96C965B
PGP Key Fingerprint: 3EC2 7B68 B072 B65C 9044 BE9C 07B7 E916 BDE5 AC10
PGP Key: https://www.us-cert.gov/pgp/soc.asc