US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary
- December 2012 -

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

Executive Summary

During December 2012, US-CERT issued four Current Activity entries, one Alert, and four weekly Bulletins.

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

Contents

Current Activity

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

Current Activity for December 2012	
December 3	Google Releases Google Chrome 23.0.1271.95
December 7	Microsoft Releases Advance Notification for December Security Bulletin
December 11	Microsoft Releases December 2012 Security Bulletin
December 13	Google Releases Google Chrome 23.0.1271.97

- Microsoft released updates to address vulnerabilities in Microsoft Windows, Internet Explorer, Microsoft Office, and Microsoft Server Software as part of the Microsoft Security Bulletin Summary for December 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.
- Google released updates for Google Chrome to address multiple vulnerabilities.
    - Google has released Google Chrome 23.0.1271.95 for Windows, Mac, and ChromeFrame to address vulnerabilities that could result in a denial of service or allow an attacker to execute arbitrary code. US-CERT encourages users and administrators to review the Google Chrome Release blog entry and update to Chrome 23.0.1271.95 to help mitigate the risk.

- Google has released Google Chrome 23.0.1271.97 for Windows, Mac, Linux, and ChromeFrame to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code or cause a denial of service. US-CERT encourages users and administrators to review the Google Chrome Release blog entry and update to Chrome 23.0.1271.97.

Alerts

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

Alerts for December 2012	
December 11	TA12-346A Microsoft Updates for Multiple Vulnerabilities

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 December 2012	
December 3	SB12-338 Vulnerability Summary for the Week of November 26, 2012
December 10	SB12-345 Vulnerability Summary for the Week of December 3, 2012
December 17	SB12-352 Vulnerability Summary for the Week of December 10, 2012
December 28	SB12-359 Vulnerability Summary for the Week of December 17, 2012

A total of 253 vulnerabilities were recorded in the NVD during December 2012.

Security Highlights

On December 29, 2012, US-CERT released a Vulnerability Note to notify users and administrators of the vulnerability and available workarounds.

Microsoft Internet Explorer CButton use-after-free vulnerability

Microsoft Internet Explorer contains a use-after free vulnerability in the mshtml CButton object. Specially crafted JavaScript can cause Internet Explorer to free the CButton object without removing a pointer, resulting in a state where Internet Explorer may attempt to call an invalid memory address. This memory address may be under the control of the attacker.

This vulnerability is currently being exploited in the wild, using Adobe Flash to achieve a heap spray and Java to provide Return Oriented Programming (ROP) gadgets. Other proof-of-concept exploits are publicly available that do not use heap spraying.

Further details on possible workarounds are available in the Vulnerability Note VU#154201 on the US-CERT website.

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 us at 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