Security TechCenter

Microsoft Security Bulletin Summary for November 2013

Published: Tuesday, November 12, 2013

Version: 1.0

This bulletin summary lists security bulletins released for November 2013.

With the release of the security bulletins for November 2013, this bulletin summary replaces the bulletin advance notification originally issued November 7, 2013. For more information about the bulletin advance notification service, see Microsoft Security Bulletin Advance Notification.

For information about how to receive automatic notifications whenever Microsoft security bulletins are issued, visit Microsoft Technical Security Notifications.

Microsoft is hosting a webcast to address customer questions on these bulletins on November 13, 2013, at 11:00 AM Pacific Time (US & Canada). Register now for the November Security Bulletin Webcast.

Microsoft also provides information to help customers prioritize monthly security updates with any non-security updates that are being released on the same day as the monthly security updates. Please see the section, **Other Information**.

Bulletin Information

Executive Summaries

The following table summarizes the security bulletins for this month in order of severity.

For details on affected software, see the next section, **Affected Software**.

Bulletin ID	Bulletin Title and Executive Summary	Maximum Severity Rating and Vulnerability Impact	Restart Requirement	Affected Software
MS13-088	**Cumulative Security Update for Internet Explorer (2888505)** This security update resolves ten privately reported vulnerabilities in Internet Explorer. The most severe vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer. An attacker who successfully exploited the most severe of these vulnerabilities could gain the same user rights as the current user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.	Critical Remote Code Execution	Requires restart	Microsoft Windows, Internet Explorer
MS13-089	**Vulnerability in Windows Graphics Device Interface Could Allow Remote Code Execution (2876331)** This security update resolves a privately reported vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user views or opens a specially crafted Windows Write file in WordPad. An attacker who successfully exploited this vulnerability could gain the same user rights as the current user. Users whose accounts are configured to	Critical Remote Code Execution	Requires restart	Microsoft Windows

Bulletin ID	Bulletin Title and Executive Summary	Maximum Severity Rating and Vulnerability Impact	Restart Requirement	Affected Software
	have fewer user rights on the system could be less impacted than users who operate with administrative user rights.			
MS13-090	**Cumulative Security Update of ActiveX Kill Bits (2900986)** This security update resolves a privately reported vulnerability that is currently being exploited. The vulnerability exists in the InformationCardSigninHelper Class ActiveX control. The vulnerability could allow remote code execution if a user views a specially crafted webpage with Internet Explorer, instantiating the ActiveX control. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.	Critical Remote Code Execution	May require restart	Microsoft Windows
MS13-091	**Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2885093)** This security update resolves three privately reported vulnerabilities in Microsoft Office. The vulnerabilities could allow remote code execution if a specially crafted WordPerfect document file is opened in an affected version of Microsoft Office software. An attacker who successfully exploited the most severe vulnerabilities could gain the same user rights as the current user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.	Important Remote Code Execution	May require restart	Microsoft Office
MS13-092	**Vulnerability in Hyper-V Could Allow Elevation of Privilege (2893986)** This security update resolves a privately reported vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker passes a specially crafted function parameter in a hypercall from an existing running virtual machine to the hypervisor. The vulnerability could also allow denial of service for the Hyper-V host if the attacker passes a specially crafted function parameter in a hypercall from an existing running virtual machine to the hypervisor.	Important Elevation of Privilege	Requires restart	Microsoft Windows
MS13-093	**Vulnerability in Windows Ancillary Function Driver Could Allow Information Disclosure (2875783)** This security update resolves a privately reported vulnerability in Microsoft Windows. The vulnerability could allow information disclosure if an attacker logs on to an affected system as a local user, and runs a specially crafted application on the system that is designed to enable the attacker to obtain information from a higher-privileged account. An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability.	Important Information Disclosure	Requires restart	Microsoft Windows

Bulletin ID	Bulletin Title and Executive Summary	Maximum Severity Rating and Vulnerability Impact	Restart Requirement	Affected Software
MS13-094	**Vulnerability in Microsoft Outlook Could Allow Information Disclosure (2894514)** This security update resolves a publicly disclosed vulnerability in Microsoft Outlook. The vulnerability could allow information disclosure if a user opens or previews a specially crafted email message using an affected edition of Microsoft Outlook. An attacker who successfully exploited this vulnerability could ascertain system information, such as the IP address and open TCP ports, from the target system and other systems that share the network with the target system.	Important Information Disclosure	May require restart	Microsoft Office
MS13-095	**Vulnerability in Digital Signatures Could Allow Denial of Service (2868626)** This security update resolves a privately reported vulnerability in Microsoft Windows. The vulnerability could allow denial of service when an affected web service processes a specially crafted X.509 certificate.	Important Denial of Service	Requires restart	Microsoft Windows

Top of section

Exploitability Index

Affected Software

Detection and Deployment Tools and Guidance

Other Information

Microsoft Windows Malicious Software Removal Tool

For the bulletin release that occurs on the second Tuesday of each month, Microsoft has released an updated version of the Microsoft Windows Malicious Software Removal Tool on Windows Update, Microsoft Update, Windows Server Update Services, and the Download Center. No updated version of the Microsoft Windows Malicious Software Removal Tool is available for out-of-band security bulletin releases.

Top of section

Non-Security Updates on MU, WU, and WSUS

For information about non-security releases on Windows Update and Microsoft Update, please see:

- Microsoft Knowledge Base Article 894199: Description of Software Update Services and Windows Server Update Services changes in content. Includes all Windows content.
- Updates from Past Months for Windows Server Update Services. Displays all new, revised, and rereleased updates for Microsoft products other than Microsoft Windows.

Top of section

Microsoft Active Protections Program (MAPP)

To improve security protections for customers, Microsoft provides vulnerability information to major security software providers in advance of each monthly security update release. Security software providers can then use this vulnerability information to provide updated protections to customers via their security software or devices, such as antivirus, network-based intrusion detection systems, or host-based intrusion prevention systems. To determine whether active protections are available from security software providers, please visit the active protections websites provided by program partners listed in Microsoft Active Protections Program (MAPP) Partners.

Top of section

Security Strategies and Community

Update Management Strategies

Security Guidance for Update Management provides additional information about Microsoft's best-practice recommendations for applying security updates.

Obtaining Other Security Updates

Updates for other security issues are available from the following locations:

- Security updates are available from Microsoft Download Center. You can find them most easily by doing a keyword search for "security update".
- Updates for consumer platforms are available from Microsoft Update.
- You can obtain the security updates offered this month on Windows Update, from Download Center on Security and Critical Releases ISO CD Image files. For more information, see Microsoft Knowledge Base Article 913086.

IT Pro Security Community

Learn to improve security and optimize your IT infrastructure, and participate with other IT Pros on security topics in IT Pro Security Community.

Top of section

Acknowledgments

Microsoft thanks the following for working with us to help protect customers:

MS13-088

- Simon Zuckerbraun, working with HP's Zero Day Initiative, for reporting the Internet Explorer Memory Corruption Vulnerability (CVE-2013-3871)
- Masato Kinugawa for reporting the Internet Explorer Information Disclosure Vulnerability (CVE-2013-3908)
- Sergey Markov for reporting the Internet Explorer Information Disclosure Vulnerability (CVE-2013-3909)
- Peter 'corelanc0d3r' Van Eeckhoutte of Corelan, working with HP's Zero Day Initiative, for reporting the Internet Explorer Memory Corruption Vulnerability (CVE-2013-3910)
- Stephen Fewer of Harmony Security, working with HP's Zero Day Initiative, for reporting the Internet Explorer Memory Corruption Vulnerability (CVE-2013-3911)
- lokihardt@ASRT, working with HP's Zero Day Initiative, for reporting the Internet Explorer Memory Corruption Vulnerability (CVE-2013-3912)
- An anonymous researcher, working with VeriSign iDefense Labs, for reporting the Internet Explorer Memory Corruption Vulnerability (CVE-2013-3914)
- Bo Qu of Palo Alto Networks for reporting the Internet Explorer Memory Corruption Vulnerability (CVE-2013-3915)
- Bo Qu of Palo Alto Networks for reporting the Internet Explorer Memory Corruption Vulnerability (CVE-2013-3916)
- An anonymous researcher, working with HP's Zero Day Initiative, for reporting the Internet Explorer Memory Corruption Vulnerability (CVE-2013-3917)
- Bo Qu of Palo Alto Networks for reporting the Internet Explorer Memory Corruption Vulnerability (CVE-2013-3917)

MS13-089

- Hossein Lotfi of Secunia Research for reporting the Graphics Device Interface Integer Overflow Vulnerability (CVE-2013-3940)

MS13-090

- ucq and Daiki Fukumori of the Cyber Defense Institute, Inc. for reporting the InformationCardSigninHelper Vulnerability (CVE-2013-3918)
- iSIGHT Partners for working with us on the InformationCardSigninHelper Vulnerability (CVE-2013-3918)
- Dan Caselden and Xiaobo Chen of FireEye for working with us on the InformationCardSigninHelper Vulnerability (CVE-2013-3918)

MS13-091

- Merliton for reporting the WPD File Format Memory Corruption Vulnerability (CVE-2013-0082)
- Will Dormann of the CERT/CC for reporting the Word Stack Buffer Overwrite Vulnerability (CVE-2013-1324)
- Will Dormann of the CERT/CC for reporting the Word Heap Overwrite Vulnerability (CVE-2013-1325)

MS13-092

- Christian Weyer for reporting the Address Corruption Vulnerability (CVE-2013-3898)

MS13-094

- Alexander Klink of n.runs professionals GmbH for reporting the S/MIME AIA Vulnerability (CVE-2013-3905)

MS13-095

- James Forshaw of Context Information Security for reporting the Digital Signatures Vulnerability (CVE-2013-3869)

Top of section

Support

- The affected software listed has been tested to determine which versions are affected. Other versions are past their support life cycle. To determine the support life cycle for your software version, visit Microsoft Support Lifecycle.
- Security solutions for IT professionals: TechNet Security Troubleshooting and Support
- Help protect your computer that is running Windows from viruses and malware: Virus Solution and Security Center
- Local support according to your country: International Support

Top of section

Disclaimer

The information provided in the Microsoft Knowledge Base is provided "as is" without warranty of any kind. Microsoft disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Microsoft Corporation or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Microsoft Corporation or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Top of section

Revisions

- V1.0 (November 12, 2013): Bulletin Summary published.

Top of section

Top of page

Manage Your Profile | Contact Us | Newsletter
Terms of Use | Trademarks | Privacy Statement | Site Feedback