Avecto Whitepaper

2013 Microsoft Vulnerabilities Study: Mitigating Risk by Removing User Privileges

Analysis of Microsoft Security Bulletins from 2013 highlights that 92% of Critical vulnerabilities would be mitigated by removing admin rights across an enterprise.

Contents

Introduction

This report has been compiled by Avecto through the analysis of data from Security Bulletins issued by Microsoft throughout 2013. Microsoft bulletins are issued on the second Tuesday of each month, a date known commonly as "Patch Tuesday", and contain fixes for vulnerabilities affecting Microsoft products that have been discovered since the last bulletin's release. Network Administrators, Security Managers and IT Professionals then respond to the update as quickly as they are able, ensuring the patches are rolled out across their systems to protect against the known vulnerabilities.

October 2013 marked the ten year anniversary of these scheduled updates providing a milestone for Avecto's top line analysis of the annual figures in order to determine the vulnerability landscape and conclude the effect of removing user admin rights.

Methodology

Each bulletin issued by Microsoft contains an Executive Summary with general information regarding that bulletin. For this report, a vulnerability is classed as one that could be mitigated by removing admin rights if the sentence "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" is found within the Executive Summary of the bulletin in which that vulnerability appears.

For a more detailed overview of the methodology used to produce this report, please see Appendix 1; Detailed Methodology.

Key Findings

The report highlights the following key findings:

- Of the **147 vulnerabilities published by Microsoft in 2013** with a Critical rating, **92%** were concluded to be mitigated by removing administrator rights
- **96% of Critical vulnerabilities affecting Windows** operating systems could be mitigated by removing admin rights
- **100% of all vulnerabilities affecting Internet Explorer** could be mitigated by removing admin rights
- **91% of vulnerabilities affecting Microsoft Office** could be mitigated by removing admin rights
- **100% of Critical Remote Code Execution vulnerabilities** and 80% of Critical Information Disclosure vulnerabilities could be mitigated by removing admin rights
- **60% of all Microsoft vulnerabilities** published in 2013 could be mitigated by removing admin rights

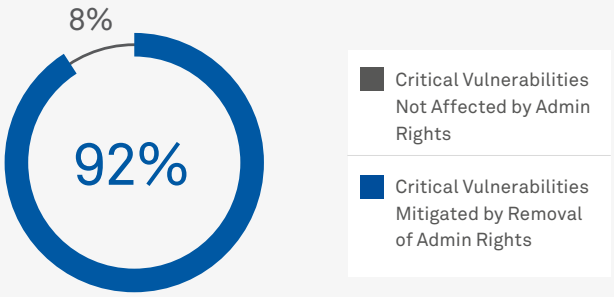
Analysis of Results

Vulnerabilities Published by Microsoft

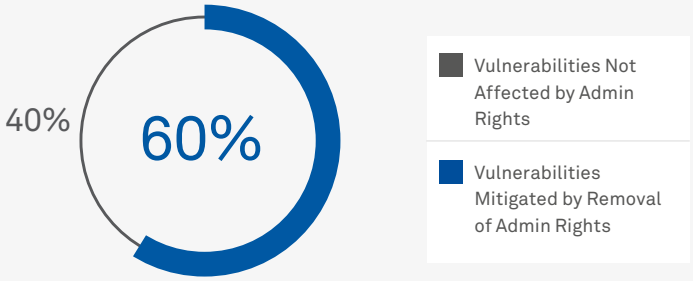
In 2013, there were 333 vulnerabilities reported in Microsoft Security Bulletins, of which 60% were found to be mitigated by removing admin rights.

Each vulnerability was rated according to severity, the most serious of which was Critical. There was a total of 147 vulnerabilities which were marked with a Critical severity rating in 2013, 92% of which were found to be mitigated by users with standard accounts.

Critical Microsoft Vulnerabilities Mitigated by Removal of Admin Rights



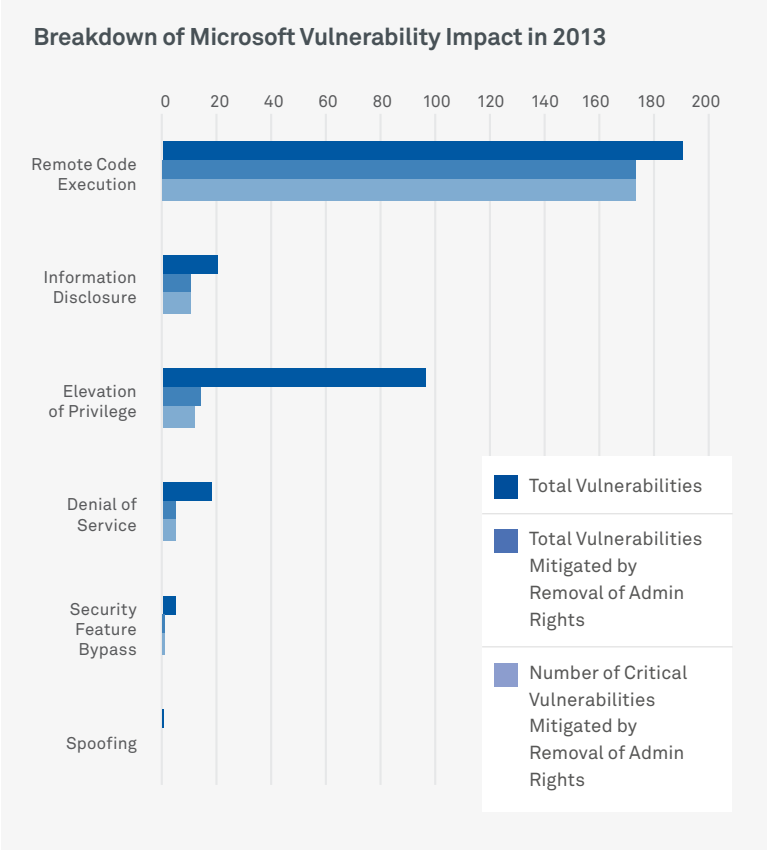
Total Microsoft Vulnerabilities Mitigated by Removal of Admin Rights



Vulnerabilities by Impact Type

Each Microsoft Security Bulletin comprises of one or more vulnerabilities, applying to one or more Microsoft products. The vulnerabilities observed in Microsoft Security Bulletins in 2013 were categorized according to their impact type: Remote Code Execution, Elevation of Privilege, Information Disclosure, Denial of Service, Security Feature Bypass, and Spoofing.

Remote Code Execution vulnerabilities account for the largest proportion of total Microsoft vulnerabilities (53%). Of these, **93% were classed as Critical and 100% of these Critical updates could be mitigated by removal of admin rights.**



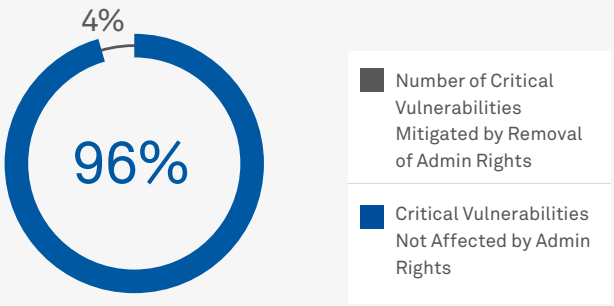
Vulnerability Analysis by Product

Windows Operating Systems

In 2013, 252 vulnerabilities were reported in Microsoft Security Bulletins affecting Windows XP, Vista, Windows 7 and Windows 8 operating systems. 54% of these vulnerabilities were classified as Critical.

Over **96% of these Critical Windows vulnerabilities** could be mitigated by the removal of admin rights.

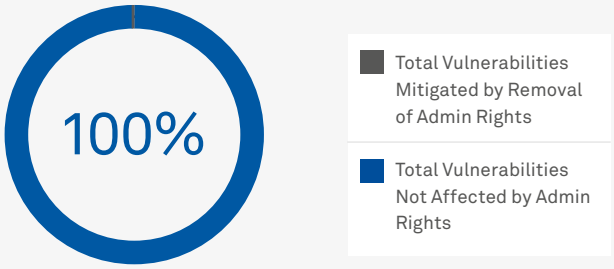
Critical Windows Vulnerabilities Mitigated by Removal of Admin Rights in 2013



Internet Explorer

In 2013, a total of 123 vulnerabilities were reported in Microsoft Security Bulletins that affected Internet Explorer (IE) versions 6-11. 100% of these IE vulnerabilities could be mitigated by the removal of user admin rights.

Total Internet Explorer Vulnerabilities Mitigated by Removal of Admin Rights in 2013

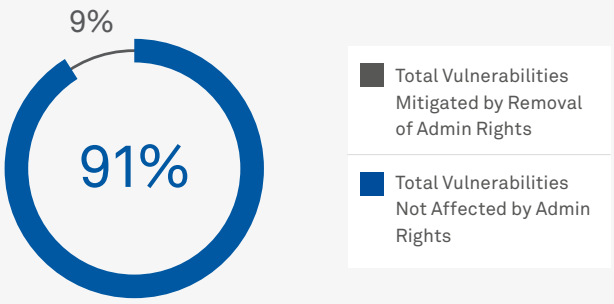


Microsoft Office

In 2013, 46 vulnerabilities were published in Microsoft Security Bulletins affecting Microsoft Office products.

This encompasses Office 2003, Office 2010, Outlook 2007, Outlook 2010, Outlook 2013, Microsoft Excel, Word, PowerPoint and Publisher. Removing admin rights would mitigate 91% of these Office vulnerabilities and over 83% of Office vulnerabilities with a rating of Critical.

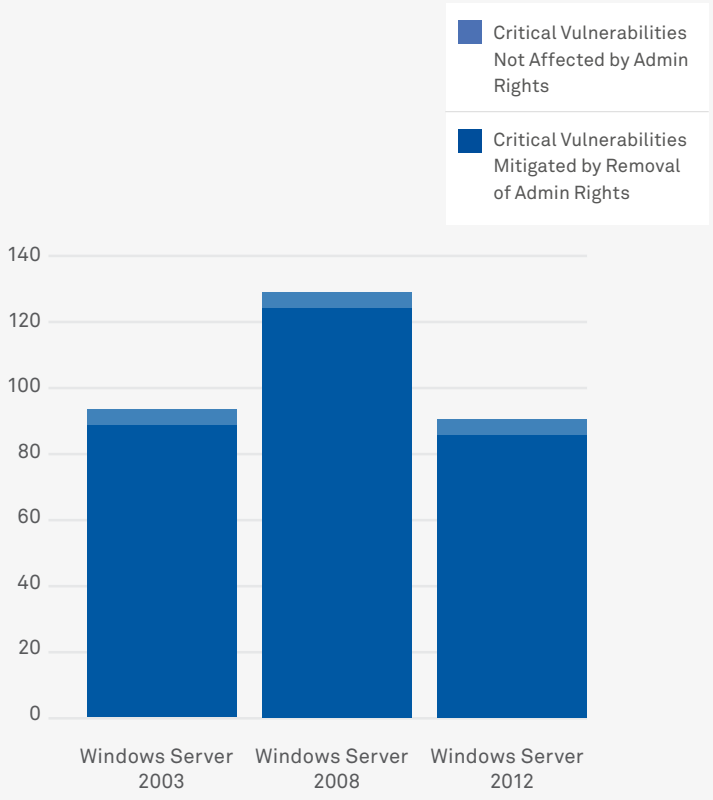
Total Internet Explorer Vulnerabilities Mitigated by Removal of Admin Rights in 2013



Windows Server

252 vulnerabilities were reported in Microsoft Security Bulletins affecting Microsoft Windows Server in 2013. Of the 136 vulnerabilities with a Critical rating, 96% were found to be mitigated by the removal of admin rights.

Critical Windows Server Vulnerabilities Mitigated by Removal of Admin Rights



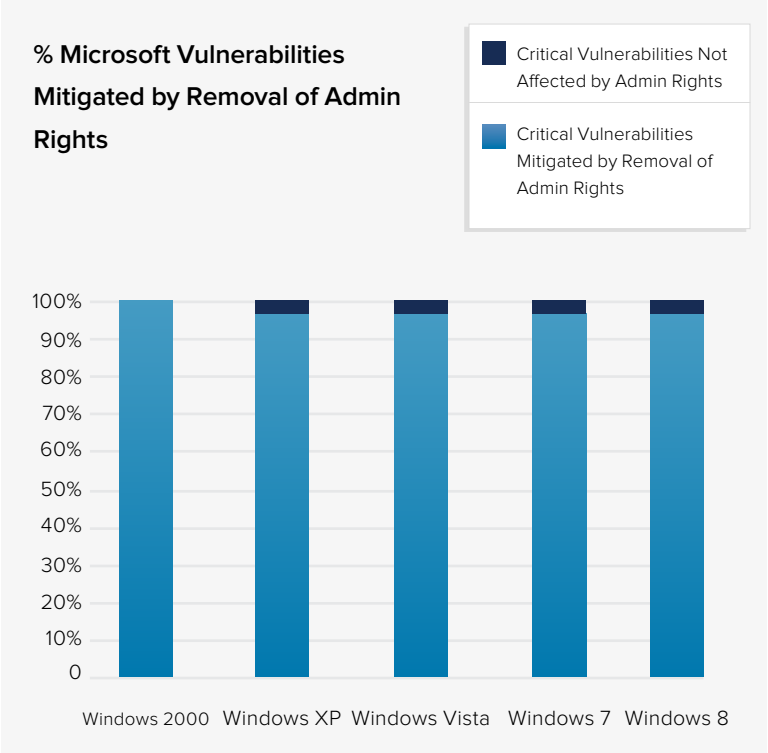
Microsoft Vulnerabilities Report 2013: Examining the Impact of XP

In the wake of Microsoft's withdrawal of support for its XP Operating System, we set out to take a brief look at the impact of XP vulnerabilities on the original Microsoft Vulnerabilities Report. While the original analysis was conducted before XP entered end-of-life, the aim was to establish whether vulnerabilities in XP had affected the overall findings significantly.

The report found that over 96% of Critical vulnerabilities in Windows Operating Systems could be mitigated by removing administrative rights. This figure was calculated based on all vulnerabilities applicable to all Windows operating systems, removing duplications.

But what happens when you take out the legacy XP solution?

As demonstrated in the chart below, the analysis found that removing the XP vulnerabilities from the report has negligible difference on the overall findings.



The message remains clear: Removal of administrative rights is an essential strategy for overcoming security vulnerabilities.

We would urge all businesses, even those that have migrated away from XP to the newer platforms of Windows 7/8 to adopt an approach of least privilege, using an appropriate privilege management

Conclusion

Analysis of Microsoft Security Bulletins in 2013 has highlighted a significant number of vulnerabilities which could be mitigated by the removal of user admin rights. Awareness of the importance of removing user admin rights is growing, with increasing internal and external security risks faced by today's modern enterprises. Analysts and experts commonly acknowledge that removing user admin rights is one of the most important steps a business can take in increasing its security defenses and dramatically reducing risk of malware infection.

About Avecto

Avecto is a pioneering security software company with a vision to transform business cultures, freeing all users to be creative, productive and profitable. Established in 2008 by UK entrepreneurs Paul Kenyon and Mark Austin, Avecto is headquartered in Manchester (UK) with a network of global partners and offices in Boston (US), and Melbourne (Australia).

Through constant innovation, Avecto combines the technologies of privilege management, application control and sandboxing to create Defendpoint; proactive endpoint security software that protects against unknown cyber threats.

Avecto's consultative approach delivers technical solutions to commercial challenges; empowering global enterprises to strike just the right balance between security defense in depth and user flexibility.

SC Magazine Awards 2013 Europe Winner

2013 Computing Security Awards Winner New Product of the Year

Deloitte. Technology Fast50 UK 2013

Microsoft Partner Gold Application Development

UK

Hobart House
Cheadle Royal Business Park
Cheadle, Cheshire, SK8 3SR

Phone +44 (0) 845 519 0114
Fax +44 (0) 845 519 0115

Americas

125 Cambridge Park Drive
Suite 301, Cambridge, MA 02140
USA

Phone 978 703 4169
Fax 978 910 0448

Australia

Level 8
350 Collins Street, Melbourne,
Victoria 3000, Australia

Phone +613 8605 4822
Fax +613 8601 1180

Avecto
@avecto
+Avecto
avecto.com
info@avecto.com

Appendix 1: Detailed Methodology

Data source

This report has been compiled following analysis of the Security bulletins published in 2013 by Microsoft. Each bulletin issued contains an Executive Summary with general information regarding that bulletin. If the sentence "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" is contained within the Executive Summary, it is assumed that all vulnerabilities within that bulletin could be mitigated by removing admin rights from users.

N.B: There is no vulnerability-specific information on privilege mitigation within the bulletin.

Bulletins & vulnerabilities

Each bulletin comprises of one or more vulnerabilities, applying to one or more Microsoft products. This is shown as a matrix on each bulletin page.

Each individual vulnerability has an impact type, which in 2013 fell into 6 categories: Remote Code Execution, Elevation of Privilege, Information Disclosure, Denial of Service, Security Feature Bypass and Spoofing. These can occasionally vary for each individual vulnerability, depending on the software or combination of software affected.

A vulnerability of each type often applies to a combination of different versions of a product or products, and sometimes all versions – e.g. all versions of Windows clients. Not all vulnerabilities within each bulletin apply to all products or all versions of products, and often a vulnerability will only apply to a combination of products – e.g. Internet Explorer 7 on Windows XP SP2.

Each vulnerability is also assigned an aggregate severity rating by Microsoft – Critical, Important, Moderate – which also varies depending on each individual piece of software or combination of software affected.

Certain vulnerabilities have appeared in multiple bulletins throughout 2013, usually affecting different software. In these cases, the vulnerability itself is only counted once, with all affected software types attributed to that one entry for the benefit of clarity and removal of duplication.

Accuracy of vulnerability data

A number of generalizations have been made for each vulnerability as follows:

- Each vulnerability was classified with the highest severity rating of all instances of that vulnerability where it appeared multiple times.
- Each vulnerability was classified with the most prevalent type for all instances of that vulnerability.
- Product versions were not taken into account.
- Product combinations were not taken into account.
- Vulnerabilities to certain software were also considered a vulnerability to the edition of Windows named as a combination. E.g. a vulnerability for "Internet Explorer 6 for Windows XP Service Pack 3" is taken as a vulnerability for **Internet Explorer 6** and **Windows XP**.

Appendix 2: Raw data

The data to produce this report has been compiled from publically available data issued by Microsoft which can be accessed here: http://technet.microsoft.com/en-us/security/dn481339.

While we have made every effort to ensure the accuracy of information, Avecto Limited cannot be held responsible for any errors or omissions in the data.

Summary of Bulletins from 2013

Bulletin ID	Date	Vulnerability	Impact	Severity	Mitigated by Standard Rights
MS13-001	08/01/2013	CVE-2013-0011	Remote Code Execution	Critical	No
MS13-002	08/01/2013	CVE-2013-0006	Remote Code Execution	Critical	Yes
MS13-002	08/01/2013	CVE-2013-0007	Remote Code Execution	Critical	Yes
MS13-003	08/01/2013	CVE-2013-0009	Elevation of Privilege	Important	No
MS13-003	08/01/2013	CVE-2013-0010	Elevation of Privilege	Important	No
MS13-004	08/01/2013	CVE-2013-0001	Information Disclosure	Moderate	Yes
MS13-004	08/01/2013	CVE-2013-0002	Elevation of Privilege	Important	Yes
MS13-004	08/01/2013	CVE-2013-0003	Elevation of Privilege	Important	Yes
MS13-004	08/01/2013	CVE-2013-0004	Elevation of Privilege	Important	Yes
MS13-005	08/01/2013	CVE-2013-0008	Elevation of Privilege	Important	Yes
MS13-006	08/01/2013	CVE-2013-0013	Security Feature Bypass	Important	No
MS13-007	08/01/2013	CVE-2013-0005	Denial of Service	Important	No
MS13-008	14/01/2013	CVE-2012-4792	Remote Code Execution	Critical	Yes
MS13-009	12/02/2013	CVE-2013-0015	Information Disclosure	Important	Yes
MS13-009	12/02/2013	CVE-2013-0018	Remote Code Execution	Critical	Yes
MS13-009	12/02/2013	CVE-2013-0019	Remote Code Execution	Critical	Yes
MS13-009	12/02/2013	CVE-2013-0020	Remote Code Execution	Critical	Yes
MS13-009	12/02/2013	CVE-2013-0021	Remote Code Execution	Critical	Yes
MS13-009	12/02/2013	CVE-2013-0022	Remote Code Execution	Critical	Yes
MS13-009	12/02/2013	CVE-2013-0023	Remote Code Execution	Critical	Yes
MS13-009	12/02/2013	CVE-2013-0024	Remote Code Execution	Critical	Yes
MS13-009	12/02/2013	CVE-2013-0025	Remote Code Execution	Critical	Yes
MS13-009	12/02/2013	CVE-2013-0026	Remote Code Execution	Critical	Yes
MS13-009	12/02/2013	CVE-2013-0027	Remote Code Execution	Critical	Yes
MS13-009	12/02/2013	CVE-2013-0028	Remote Code Execution	Critical	Yes
MS13-009	12/02/2013	CVE-2013-0029	Remote Code Execution	Critical	Yes

Bulletin ID	Date	Vulnerability	Impact	Severity	Mitigated by Standard Rights
MS13-010	12/02/2013	CVE-2013-0030	Remote Code Execution	Critical	Yes
MS13-011	12/02/2013	CVE-2013-0077	Remote Code Execution	Critical	Yes
MS13-012	12/02/2013	CVE-2013-0393	Denial of Service	Important	No
MS13-012	12/02/2013	CVE-2013-0418	Remote Code Execution	Critical	No
MS13-013	12/02/2013	CVE-2012-3214	Remote Code Execution	Important	No
MS13-013	12/02/2013	CVE-2012-3217	Remote Code Execution	Important	No
MS13-014	12/02/2013	CVE-2013-1281	Denial of Service	Important	No
MS13-015	12/02/2013	CVE-2013-0073	Elevation of Privilege	Important	Yes
MS13-016	12/02/2013	CVE-2013-1248	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1249	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1250	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1251	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1252	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1253	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1254	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1255	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1256	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1257	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1258	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1259	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1260	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1261	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1262	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1263	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1264	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1265	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1266	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1267	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1268	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1269	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1270	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1271	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1272	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1273	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1274	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1275	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1276	Elevation of Privilege	Important	No
MS13-016	12/02/2013	CVE-2013-1277	Elevation of Privilege	Important	No

Bulletin ID	Date	Vulnerability	Impact	Severity	Mitigated by Standard Rights
MS13-017	12/02/2013	CVE-2013-1278	Elevation of Privilege	Important	No
MS13-017	12/02/2013	CVE-2013-1279	Elevation of Privilege	Important	No
MS13-017	12/02/2013	CVE-2013-1280	Elevation of Privilege	Important	No
MS13-018	12/02/2013	CVE-2013-0075	Denial of Service	Important	No
MS13-019	12/02/2013	CVE-2013-0076	Elevation of Privilege	Important	No
MS13-020	12/02/2013	CVE-2013-1313	Remote Code Execution	Critical	Yes
MS13-021	12/03/2013	CVE-2013-0087	Remote Code Execution	Critical	Yes
MS13-021	12/03/2013	CVE-2013-0088	Remote Code Execution	Critical	Yes
MS13-021	12/03/2013	CVE-2013-0089	Remote Code Execution	Critical	Yes
MS13-021	12/03/2013	CVE-2013-0090	Remote Code Execution	Critical	Yes
MS13-021	12/03/2013	CVE-2013-0091	Remote Code Execution	Critical	Yes
MS13-021	12/03/2013	CVE-2013-0092	Remote Code Execution	Critical	Yes
MS13-021	12/03/2013	CVE-2013-0093	Remote Code Execution	Critical	Yes
MS13-021	12/03/2013	CVE-2013-0094	Remote Code Execution	Critical	Yes
MS13-021	12/03/2013	CVE-2013-1288	Remote Code Execution	Critical	Yes
MS13-022	12/03/2013	CVE-2013-0074	Remote Code Execution	Critical	Yes
MS13-023	12/03/2013	CVE-2013-0079	Remote Code Execution	Critical	Yes
MS13-024	12/03/2013	CVE-2013-0080	Elevation of Privilege	Important	No
MS13-024	12/03/2013	CVE-2013-0083	Elevation of Privilege	Critical	No
MS13-024	12/03/2013	CVE-2013-0084	Elevation of Privilege	Important	No
MS13-024	12/03/2013	CVE-2013-0085	Denial of Service	Moderate	No
MS13-025	12/03/2013	CVE-2013-0086	Information Disclosure	Important	No
MS13-026	12/03/2013	CVE-2013-0095	Information Disclosure	Important	No
MS13-027	12/03/2013	CVE-2013-1285	Elevation of Privilege	Important	No
MS13-027	12/03/2013	CVE-2013-1286	Elevation of Privilege	Important	No
MS13-027	12/03/2013	CVE-2013-1287	Elevation of Privilege	Important	No
MS13-028	09/04/2013	CVE-2013-1303	Remote Code Execution	Critical	Yes
MS13-028	09/04/2013	CVE-2013-1304	Remote Code Execution	Critical	Yes
MS13-028	09/04/2013	CVE-2013-1338	Remote Code Execution	Critical	Yes
MS13-029	09/04/2013	CVE-2013-1296	Remote Code Execution	Critical	Yes
MS13-030	09/04/2013	CVE-2013-1290	Information Disclosure	Important	No
MS13-031	09/04/2013	CVE-2013-1284	Elevation of Privilege	Important	No
MS13-031	09/04/2013	CVE-2013-1294	Elevation of Privilege	Important	No
MS13-032	09/04/2013	CVE-2013-1282	Denial of Service	Important	No
MS13-033	09/04/2013	CVE-2013-1295	Elevation of Privilege	Important	No
MS13-034	09/04/2013	CVE-2013-0078	Elevation of Privilege	Important	No
MS13-035	09/04/2013	CVE-2013-1289	Elevation of Privilege	Important	No
MS13-036	09/04/2013	CVE-2013-1283	Elevation of Privilege	Important	No

Bulletin ID	Date	Vulnerability	Impact	Severity	Mitigated by Standard Rights
MS13-036	09/04/2013	CVE-2013-1291	Denial of Service	Moderate	No
MS13-036	09/04/2013	CVE-2013-1292	Elevation of Privilege	Important	No
MS13-036	09/04/2013	CVE-2013-1293	Elevation of Privilege	Moderate	No
MS13-037	14/05/2013	CVE-2013-0811	Remote Code Execution	Critical	Yes
MS13-037	14/05/2013	CVE-2013-1297	Information Disclosure	Important	Yes
MS13-037	14/05/2013	CVE-2013-1306	Remote Code Execution	Critical	Yes
MS13-037	14/05/2013	CVE-2013-1307	Remote Code Execution	Critical	Yes
MS13-037	14/05/2013	CVE-2013-1308	Remote Code Execution	Critical	Yes
MS13-037	14/05/2013	CVE-2013-1309	Remote Code Execution	Critical	Yes
MS13-037	14/05/2013	CVE-2013-1310	Remote Code Execution	Critical	Yes
MS13-037	14/05/2013	CVE-2013-1311	Remote Code Execution	Critical	Yes
MS13-037	14/05/2013	CVE-2013-1312	Remote Code Execution	Critical	Yes
MS13-037	14/05/2013	CVE-2013-2551	Remote Code Execution	Critical	Yes
MS13-037	14/05/2013	CVE-2013-3140	Remote Code Execution	Critical	Yes
MS13-038	14/05/2013	CVE-2013-1347	Remote Code Execution	Critical	Yes
MS13-039	14/05/2013	CVE-2013-1305	Denial of Service	Important	No
MS13-040	14/05/2013	CVE-2013-1336	Spoofing	Important	No
MS13-040	14/05/2013	CVE-2013-1337	Security Feature Bypass	Important	No
MS13-041	14/05/2013	CVE-2013-1302	Remote Code Execution	Important	Yes
MS13-042	14/05/2013	CVE-2013-1316	Remote Code Execution	Important	Yes
MS13-042	14/05/2013	CVE-2013-1317	Remote Code Execution	Important	Yes
MS13-042	14/05/2013	CVE-2013-1318	Remote Code Execution	Important	Yes
MS13-042	14/05/2013	CVE-2013-1319	Remote Code Execution	Important	Yes
MS13-042	14/05/2013	CVE-2013-1320	Remote Code Execution	Important	Yes
MS13-042	14/05/2013	CVE-2013-1321	Remote Code Execution	Important	Yes
MS13-042	14/05/2013	CVE-2013-1322	Remote Code Execution	Important	Yes
MS13-042	14/05/2013	CVE-2013-1323	Remote Code Execution	Important	Yes
MS13-042	14/05/2013	CVE-2013-1327	Remote Code Execution	Important	Yes
MS13-042	14/05/2013	CVE-2013-1328	Remote Code Execution	Important	Yes
MS13-042	14/05/2013	CVE-2013-1329	Remote Code Execution	Important	Yes
MS13-043	14/05/2013	CVE-2013-1335	Remote Code Execution	Important	Yes
MS13-044	14/05/2013	CVE-2013-1301	Information Disclosure	Important	No
MS13-045	14/05/2013	CVE-2013-0096	Information Disclosure	Important	No
MS13-046	14/05/2013	CVE-2013-1332	Elevation of Privilege	Important	No
MS13-046	14/05/2013	CVE-2013-1333	Elevation of Privilege	Important	No
MS13-046	14/05/2013	CVE-2013-1334	Elevation of Privilege	Important	No
MS13-047	11/06/2013	CVE-2013-3110	Remote Code Execution	Critical	Yes
MS13-047	11/06/2013	CVE-2013-3111	Remote Code Execution	Critical	Yes
MS13-047	11/06/2013	CVE-2013-3112	Remote Code Execution	Critical	Yes

Bulletin ID	Date	Vulnerability	Impact	Severity	Mitigated by Standard Rights
MS13-047	11/06/2013	CVE-2013-3113	Remote Code Execution	Critical	Yes
MS13-047	11/06/2013	CVE-2013-3114	Remote Code Execution	Critical	Yes
MS13-047	11/06/2013	CVE-2013-3116	Remote Code Execution	Critical	Yes
MS13-047	11/06/2013	CVE-2013-3117	Remote Code Execution	Critical	Yes
MS13-047	11/06/2013	CVE-2013-3118	Remote Code Execution	Critical	Yes
MS13-047	11/06/2013	CVE-2013-3119	Remote Code Execution	Critical	Yes
MS13-047	11/06/2013	CVE-2013-3120	Remote Code Execution	Critical	Yes
MS13-047	11/06/2013	CVE-2013-3121	Remote Code Execution	Critical	Yes
MS13-047	11/06/2013	CVE-2013-3122	Remote Code Execution	Critical	Yes
MS13-047	11/06/2013	CVE-2013-3123	Remote Code Execution	Critical	Yes
MS13-047	11/06/2013	CVE-2013-3124	Remote Code Execution	Critical	Yes
MS13-047	11/06/2013	CVE-2013-3125	Remote Code Execution	Critical	Yes
MS13-047	11/06/2013	CVE-2013-3126	Remote Code Execution	Moderate	Yes
MS13-047	11/06/2013	CVE-2013-3139	Remote Code Execution	Critical	Yes
MS13-047	11/06/2013	CVE-2013-3141	Remote Code Execution	Critical	Yes
MS13-047	11/06/2013	CVE-2013-3142	Remote Code Execution	Critical	Yes
MS13-048	11/06/2013	CVE-2013-3136	Information Disclosure	Important	No
MS13-049	11/06/2013	CVE-2013-3138	Denial of Service	Important	No
MS13-050	11/06/2013	CVE-2013-1339	Elevation of Privilege	Important	No
MS13-051	11/06/2013	CVE-2013-1331	Remote Code Execution	Important	Yes
MS13-052	09/07/2013	CVE-2013-3131	Remote Code Execution	Critical	Yes
MS13-052	09/07/2013	CVE-2013-3132	Elevation of Privilege	Critical	Yes
MS13-052	09/07/2013	CVE-2013-3133	Elevation of Privilege	Important	Yes
MS13-052	09/07/2013	CVE-2013-3134	Remote Code Execution	Critical	Yes
MS13-052	09/07/2013	CVE-2013-3171	Elevation of Privilege	Important	Yes
MS13-052	09/07/2013	CVE-2013-3178	Remote Code Execution	Important	Yes
MS13-053	09/07/2013	CVE-2013-1300	Elevation of Privilege	Important	No
MS13-053	09/07/2013	CVE-2013-1340	Elevation of Privilege	Important	No
MS13-053	09/07/2013	CVE-2013-1345	Elevation of Privilege	Important	No
MS13-053	09/07/2013	CVE-2013-3167	Elevation of Privilege	Important	No
MS13-053	09/07/2013	CVE-2013-3172	Denial of Service	Moderate	No
MS13-053	09/07/2013	CVE-2013-3173	Elevation of Privilege	Important	No
MS13-053	09/07/2013	CVE-2013-3660	Remote Code Execution	Critical	No
MS13-054	09/07/2013	CVE-2013-3129	Remote Code Execution	Critical	Yes
MS13-055	09/07/2013	CVE-2013-3115	Remote Code Execution	Critical	Yes
MS13-055	09/07/2013	CVE-2013-3143	Remote Code Execution	Critical	Yes
MS13-055	09/07/2013	CVE-2013-3144	Remote Code Execution	Critical	Yes
MS13-055	09/07/2013	CVE-2013-3145	Remote Code Execution	Critical	Yes
MS13-055	09/07/2013	CVE-2013-3146	Remote Code Execution	Critical	Yes

Bulletin ID	Date	Vulnerability	Impact	Severity	Mitigated by Standard Rights
MS13-055	09/07/2013	CVE-2013-3147	Remote Code Execution	Critical	Yes
MS13-055	09/07/2013	CVE-2013-3148	Remote Code Execution	Critical	Yes
MS13-055	09/07/2013	CVE-2013-3149	Remote Code Execution	Critical	Yes
MS13-055	09/07/2013	CVE-2013-3150	Remote Code Execution	Critical	Yes
MS13-055	09/07/2013	CVE-2013-3151	Remote Code Execution	Critical	Yes
MS13-055	09/07/2013	CVE-2013-3152	Remote Code Execution	Critical	Yes
MS13-055	09/07/2013	CVE-2013-3153	Remote Code Execution	Critical	Yes
MS13-055	09/07/2013	CVE-2013-3161	Remote Code Execution	Critical	Yes
MS13-055	09/07/2013	CVE-2013-3162	Remote Code Execution	Critical	Yes
MS13-055	09/07/2013	CVE-2013-3163	Remote Code Execution	Critical	Yes
MS13-055	09/07/2013	CVE-2013-3164	Remote Code Execution	Critical	Yes
MS13-055	09/07/2013	CVE-2013-3166	Remote Code Execution	Important	Yes
MS13-055	09/07/2013	CVE-2013-3846	Remote Code Execution	Critical	Yes
MS13-056	09/07/2013	CVE-2013-3174	Remote Code Execution	Critical	Yes
MS13-057	09/07/2013	CVE-2013-3127	Remote Code Execution	Critical	Yes
MS13-058	09/07/2013	CVE-2013-3154	Elevation of Privilege	Important	No
MS13-059	13/08/2013	CVE-2013-3184	Remote Code Execution	Critical	Yes
MS13-059	13/08/2013	CVE-2013-3186	Elevation of Privilege	Moderate	Yes
MS13-059	13/08/2013	CVE-2013-3187	Remote Code Execution	Critical	Yes
MS13-059	13/08/2013	CVE-2013-3188	Remote Code Execution	Critical	Yes
MS13-059	13/08/2013	CVE-2013-3189	Remote Code Execution	Critical	Yes
MS13-059	13/08/2013	CVE-2013-3190	Remote Code Execution	Critical	Yes
MS13-059	13/08/2013	CVE-2013-3191	Remote Code Execution	Critical	Yes
MS13-059	13/08/2013	CVE-2013-3192	Information Disclosure	Moderate	Yes
MS13-059	13/08/2013	CVE-2013-3193	Remote Code Execution	Critical	Yes
MS13-059	13/08/2013	CVE-2013-3194	Remote Code Execution	Critical	Yes
MS13-059	13/08/2013	CVE-2013-3199	Remote Code Execution	Critical	Yes
MS13-060	13/08/2013	CVE-2013-3181	Remote Code Execution	Critical	Yes
MS13-061	13/08/2013	CVE-2013-2393	Remote Code Execution	Critical	No
MS13-061	13/08/2013	CVE-2013-3776	Remote Code Execution	Critical	No
MS13-061	13/08/2013	CVE-2013-3781	Remote Code Execution	Critical	No
MS13-062	13/08/2013	CVE-2013-3175	Elevation of Privilege	Important	No
MS13-063	13/08/2013	CVE-2013-2556	Security Feature Bypass	Important	No
MS13-063	13/08/2013	CVE-2013-3196	Elevation of Privilege	Important	No
MS13-063	13/08/2013	CVE-2013-3197	Elevation of Privilege	Important	No
MS13-063	13/08/2013	CVE-2013-3198	Elevation of Privilege	Important	No
MS13-064	13/08/2013	CVE-2013-3182	Denial of Service	Important	No
MS13-065	13/08/2013	CVE-2013-3183	Denial of Service	Important	No
MS13-066	13/08/2013	CVE-2013-3185	Information Disclosure	Important	No

Bulletin ID	Date	Vulnerability	Impact	Severity	Mitigated by Standard Rights
MS13-067	10/09/2013	CVE-2013-0081	Denial of Service	Important	Yes
MS13-067	10/09/2013	CVE-2013-1330	Remote Code Execution	Critical	Yes
MS13-067	10/09/2013	CVE-2013-3179	Elevation of Privilege	Important	Yes
MS13-067	10/09/2013	CVE-2013-3180	Elevation of Privilege	Important	Yes
MS13-067	10/09/2013	CVE-2013-1315	Remote Code Execution	Important	Yes
MS13-067	10/09/2013	CVE-2013-3847	Remote Code Execution	Important	Yes
MS13-067	10/09/2013	CVE-2013-3848	Remote Code Execution	Important	Yes
MS13-067	10/09/2013	CVE-2013-3849	Remote Code Execution	Important	Yes
MS13-067	10/09/2013	CVE-2013-3857	Remote Code Execution	Important	Yes
MS13-067	10/09/2013	CVE-2013-3858	Remote Code Execution	Important	Yes
MS13-068	10/09/2013	CVE-2013-3870	Remote Code Execution	Critical	Yes
MS13-069	10/09/2013	CVE-2013-3201	Remote Code Execution	Critical	Yes
MS13-069	10/09/2013	CVE-2013-3202	Remote Code Execution	Critical	Yes
MS13-069	10/09/2013	CVE-2013-3203	Remote Code Execution	Critical	Yes
MS13-069	10/09/2013	CVE-2013-3204	Remote Code Execution	Critical	Yes
MS13-069	10/09/2013	CVE-2013-3205	Remote Code Execution	Critical	Yes
MS13-069	10/09/2013	CVE-2013-3206	Remote Code Execution	Critical	Yes
MS13-069	10/09/2013	CVE-2013-3207	Remote Code Execution	Critical	Yes
MS13-069	10/09/2013	CVE-2013-3208	Remote Code Execution	Critical	Yes
MS13-069	10/09/2013	CVE-2013-3209	Remote Code Execution	Critical	Yes
MS13-069	10/09/2013	CVE-2013-3845	Remote Code Execution	Critical	Yes
MS13-070	10/09/2013	CVE-2013-3863	Remote Code Execution	Critical	Yes
MS13-071	10/09/2013	CVE-2013-0810	Remote Code Execution	Important	Yes
MS13-072	10/09/2013	CVE-2013-3160	Information Disclosure	Important	Yes
MS13-072	10/09/2013	CVE-2013-3850	Remote Code Execution	Important	Yes
MS13-072	10/09/2013	CVE-2013-3851	Remote Code Execution	Important	Yes
MS13-072	10/09/2013	CVE-2013-3852	Remote Code Execution	Important	Yes
MS13-072	10/09/2013	CVE-2013-3853	Remote Code Execution	Important	Yes
MS13-072	10/09/2013	CVE-2013-3854	Remote Code Execution	Important	Yes
MS13-072	10/09/2013	CVE-2013-3855	Remote Code Execution	Important	Yes
MS13-072	10/09/2013	CVE-2013-3856	Remote Code Execution	Important	Yes
MS13-073	10/09/2013	CVE-2013-3158	Remote Code Execution	Important	Yes
MS13-073	10/09/2013	CVE-2013-3159	Information Disclosure	Important	Yes
MS13-074	10/09/2013	CVE-2013-3155	Remote Code Execution	Important	Yes
MS13-074	10/09/2013	CVE-2013-3156	Remote Code Execution	Important	Yes
MS13-074	10/09/2013	CVE-2013-3157	Remote Code Execution	Important	Yes
MS13-075	10/09/2013	CVE-2013-3859	Elevation of Privilege	Important	No
MS13-076	10/09/2013	CVE-2013-1341	Elevation of Privilege	Important	No
MS13-076	10/09/2013	CVE-2013-1342	Elevation of Privilege	Important	No

Bulletin ID	Date	Vulnerability	Impact	Severity	Mitigated by Standard Rights
MS13-076	10/09/2013	CVE-2013-1343	Elevation of Privilege	Important	No
MS13-076	10/09/2013	CVE-2013-1344	Elevation of Privilege	Important	No
MS13-076	10/09/2013	CVE-2013-3864	Elevation of Privilege	Important	No
MS13-076	10/09/2013	CVE-2013-3865	Elevation of Privilege	Important	No
MS13-076	10/09/2013	CVE-2013-3866	Elevation of Privilege	Important	No
MS13-077	10/09/2013	CVE-2013-3862	Elevation of Privilege	Important	No
MS13-078	10/09/2013	CVE-2013-3137	Information Disclosure	Important	No
MS13-079	10/09/2013	CVE-2013-3868	Denial of Service	Important	No
MS13-080	08/10/2013	CVE-2013-3872	Remote Code Execution	Critical	Yes
MS13-080	08/10/2013	CVE-2013-3873	Remote Code Execution	Critical	Yes
MS13-080	08/10/2013	CVE-2013-3874	Remote Code Execution	Critical	Yes
MS13-080	08/10/2013	CVE-2013-3875	Remote Code Execution	Critical	Yes
MS13-080	08/10/2013	CVE-2013-3882	Remote Code Execution	Critical	Yes
MS13-080	08/10/2013	CVE-2013-3885	Remote Code Execution	Critical	Yes
MS13-080	08/10/2013	CVE-2013-3886	Remote Code Execution	Critical	Yes
MS13-080	08/10/2013	CVE-2013-3893	Remote Code Execution	Critical	Yes
MS13-080	08/10/2013	CVE-2013-3897	Remote Code Execution	Critical	Yes
MS13-081	08/10/2013	CVE-2013-3200	Elevation of Privilege	Important	No
MS13-081	08/10/2013	CVE-2013-3879	Elevation of Privilege	Important	No
MS13-081	08/10/2013	CVE-2013-3880	Elevation of Privilege	Important	No
MS13-081	08/10/2013	CVE-2013-3881	Elevation of Privilege	Important	No
MS13-081	08/10/2013	CVE-2013-3888	Elevation of Privilege	Important	No
MS13-081	08/10/2013	CVE-2013-3894	Remote Code Execution	Critical	No
MS13-082	08/10/2013	CVE-2013-3128	Remote Code Execution	Critical	Yes
MS13-082	08/10/2013	CVE-2013-3860	Denial of Service	Important	Yes
MS13-082	08/10/2013	CVE-2013-3861	Denial of Service	Important	Yes
MS13-083	08/10/2013	CVE-2013-3195	Remote Code Execution	Critical	Yes
MS13-084	08/10/2013	CVE-2013-3895	Elevation of Privilege	Important	Yes
MS13-085	08/10/2013	CVE-2013-3889	Remote Code Execution	Important	Yes
MS13-085	08/10/2013	CVE-2013-3890	Remote Code Execution	Important	Yes
MS13-086	08/10/2013	CVE-2013-3891	Remote Code Execution	Important	Yes
MS13-086	08/10/2013	CVE-2013-3892	Remote Code Execution	Important	Yes
MS13-087	08/10/2013	CVE-2013-3896	Information Disclosure	Important	No
MS13-088	12/11/2013	CVE-2013-3871	Remote Code Execution	Critical	Yes
MS13-088	12/11/2013	CVE-2013-3908	Information Disclosure	Important	Yes
MS13-088	12/11/2013	CVE-2013-3909	Information Disclosure	Important	Yes
MS13-088	12/11/2013	CVE-2013-3910	Remote Code Execution	Critical	Yes
MS13-088	12/11/2013	CVE-2013-3911	Remote Code Execution	Critical	Yes
MS13-088	12/11/2013	CVE-2013-3912	Remote Code Execution	Critical	Yes

Bulletin ID	Date	Vulnerability	Impact	Severity	Mitigated by Standard Rights
MS13-088	12/11/2013	CVE-2013-3914	Remote Code Execution	Critical	Yes
MS13-088	12/11/2013	CVE-2013-3915	Remote Code Execution	Critical	Yes
MS13-088	12/11/2013	CVE-2013-3916	Remote Code Execution	Critical	Yes
MS13-088	12/11/2013	CVE-2013-3917	Remote Code Execution	Critical	Yes
MS13-089	12/11/2013	CVE-2013-3940	Remote Code Execution	Critical	Yes
MS13-090	12/11/2013	CVE-2013-3918	Remote Code Execution	Critical	Yes
MS13-091	12/11/2013	CVE-2013-0082	Remote Code Execution	Important	Yes
MS13-091	12/11/2013	CVE-2013-1324	Remote Code Execution	Important	Yes
MS13-091	12/11/2013	CVE-2013-1325	Remote Code Execution	Important	Yes
MS13-092	12/11/2013	CVE-2013-3898	Elevation of Privilege	Important	No
MS13-093	12/11/2013	CVE-2013-3887	Information Disclosure	Important	No
MS13-094	12/11/2013	CVE-2013-3905	Information Disclosure	Important	No
MS13-095	12/11/2013	CVE-2013-3869	Denial of Service	Important	No
MS13-096	10/12/2013	CVE-2013-3906	Remote Code Execution	Critical	No
MS13-097	10/12/2013	CVE-2013-5045	Elevation of Privilege	Important	Yes
MS13-097	10/12/2013	CVE-2013-5046	Elevation of Privilege	Important	Yes
MS13-097	10/12/2013	CVE-2013-5047	Remote Code Execution	Critical	Yes
MS13-097	10/12/2013	CVE-2013-5048	Remote Code Execution	Critical	Yes
MS13-097	10/12/2013	CVE-2013-5049	Remote Code Execution	Critical	Yes
MS13-097	10/12/2013	CVE-2013-5051	Remote Code Execution	Critical	Yes
MS13-097	10/12/2013	CVE-2013-5052	Remote Code Execution	Critical	Yes
MS13-098	10/12/2013	CVE-2013-3900	Remote Code Execution	Critical	No
MS13-099	10/12/2013	CVE-2013-5056	Remote Code Execution	Critical	Yes
MS13-100	10/12/2013	CVE-2013-5059	Remote Code Execution	Important	No
MS13-101	10/12/2013	CVE-2013-3899	Elevation of Privilege	Important	No
MS13-101	10/12/2013	CVE-2013-3902	Elevation of Privilege	Important	No
MS13-101	10/12/2013	CVE-2013-3903	Denial of Service	Moderate	No
MS13-101	10/12/2013	CVE-2013-3907	Elevation of Privilege	Important	No
MS13-101	10/12/2013	CVE-2013-5058	Denial of Service	Moderate	No
MS13-102	10/12/2013	CVE-2013-3878	Elevation of Privilege	Important	No
MS13-103	10/12/2013	CVE-2013-5042	Elevation of Privilege	Important	No
MS13-104	10/12/2013	CVE-2013-5054	Information Disclosure	Important	No
MS13-105	10/12/2013	CVE-2013-5763	Remote Code Execution	Critical	No
MS13-105	10/12/2013	CVE-2013-5791	Remote Code Execution	Critical	No
MS13-105	10/12/2013	CVE-2013-5072	Elevation of Privilege	Important	No
MS13-106	10/12/2013	CVE-2013-5057	Security Feature Bypass	Important	No