Avecto Report

2014 Microsoft Vulnerabilities Report

Analysis of Microsoft “Patch Tuesday” Security Bulletins from 2014 highlights that 97% of Critical Microsoft vulnerabilities would be mitigated by removing admin rights across an enterprise.

Contents

Introduction

Compiled by Avecto, this report analyses the data from Patch Tuesday Security Bulletins issued by Microsoft throughout 2014. Microsoft bulletins are typically issued on the second Tuesday of each month, a date commonly referred to as “Patch Tuesday”, and contain fixes for vulnerabilities affecting Microsoft products that have been discovered since the last bulletins 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.

The 2014 Microsoft Vulnerabilities Report is the second time Avecto has conducted this research. In 2013, the same report found a total of 147 vulnerabilities with a Critical rating where 92% could have been mitigated by removing admin rights. Comparing the two reports indicates a 63% year on year increase in the total number of Critical vulnerabilities.

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 “Customers/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.

When we talk about vulnerabilities being mitigated by admin rights removal, this refers to instances where a standard user account either nullifies the vulnerability itself or nullifies the impact of the vulnerability by preventing the exploit from gaining elevated privileges through the user. In all instances quoted, removing admin rights mitigates the risk of the vulnerability.

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

Key findings

The 2014 report highlights the following key findings:

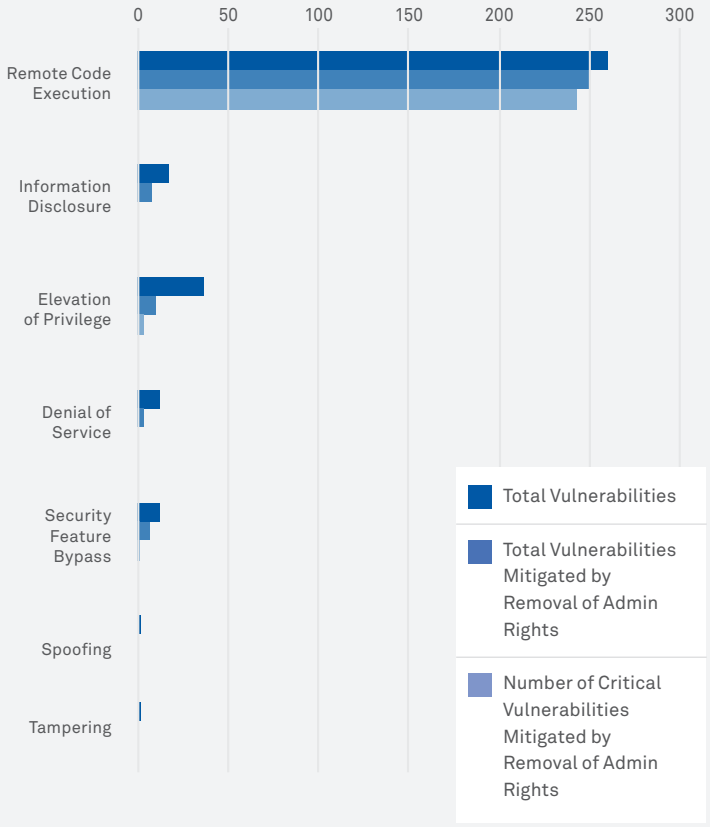
- **Of the 240 vulnerabilities published by Microsoft in 2014** with a Critical rating, **97%** were concluded to be mitigated by removing administrator rights
- There has been a **63% year on year rise** in Critical vulnerabilities since 2013
- **98% of Critical vulnerabilities affecting Windows operating systems** could be mitigated by removing admin rights
- **99.5% of all vulnerabilities in Internet Explorer** could be mitigated by removing admin rights
- **95% of vulnerabilities affecting Microsoft Office** could be mitigated by removing admin rights
- **97% of Critical Remote Code Execution** vulnerabilities could be mitigated by removing admin rights
- **80% of all Microsoft vulnerabilities** reported by us in 2014 could be mitigated by removing admin rights.

Vulnerability categories

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 2014 were categorised according to their impact type: Remote Code Execution, Elevation of Privilege, Information Disclosure, Denial of Service, Security Feature Bypass, Spoofing and Tampering.

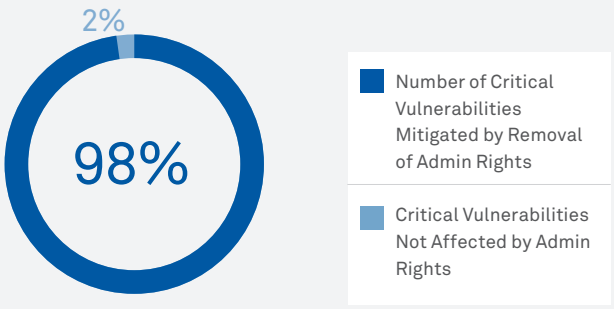
Remote Code Execution vulnerabilities account for the largest proportion of total Microsoft vulnerabilities. Of these, **93% were classed as Critical and 97% of these Critical updates could be mitigated by removal of admin rights.**

Breakdown of Microsoft Vulnerability Impact in 2014



Microsoft Windows vulnerabilities

Critical Windows Vulnerabilities Mitigated by Removal of Admin Rights in 2014



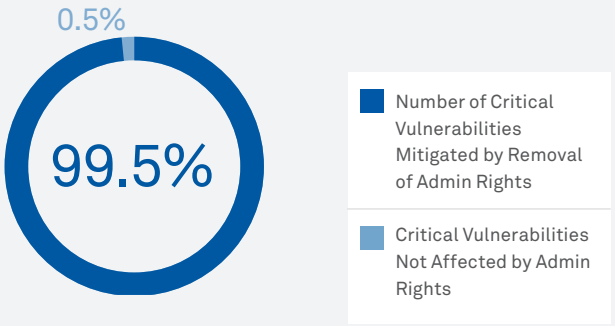
In 2014, 300 vulnerabilities were reported across Windows XP, Vista, Windows 7 and Windows 8 operating systems compared to 253 in 2013. 78% of these vulnerabilities were classified as Critical whereas just 54% were classed as Critical in 2013.

98% of Critical vulnerabilities affecting Microsoft Windows in 2014 could be mitigated by the removal of admin rights.

Internet Explorer

In 2014, a total of 245 vulnerabilities were reported that affected Internet Explorer (IE) versions 6-11, there were just 123 reported in 2013. 99.5% of IE vulnerabilities in 2014 could be mitigated by the removal of user admin rights.

Internet Explorer vulnerabilities Mitigated by Removal of Admin Rights

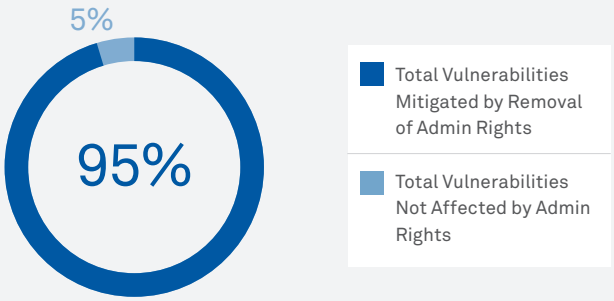


Microsoft Office

In 2014, 20 vulnerabilities were published in Microsoft Security Bulletins affecting Microsoft Office products, there were 46 vulnerabilities published in 2013.

This encompasses Office 2003, Office 2010, Outlook 2007, Outlook 2010, Outlook 2013, Microsoft Excel, Word, PowerPoint and Publisher amongst others. Removing admin rights would mitigate 95% of these Office vulnerabilities and 100% of Office vulnerabilities with a rating of Critical.

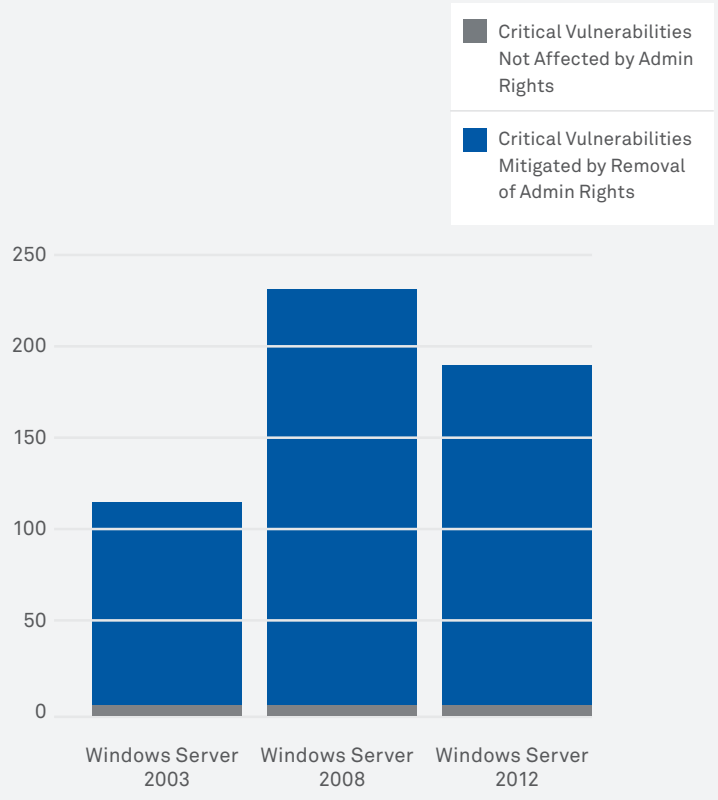
Total Windows Office Vulnerabilities in 2014



Windows Server vulnerabilities

304 vulnerabilities were reported in Microsoft Security Bulletins affecting Microsoft Windows Server in 2014, there were 252 reported in 2013. Of the 233 vulnerabilities with a Critical rating in 2014, 98% were found to be mitigated by the removal of admin rights.

Critical Windows Server Vulnerabilities Mitigated by Removal of Admin Rights



Additional Microsoft Services

Additional Microsoft Services not included in the Microsoft Office, Windows Server, Internet Explorer or Windows O/S summaries that are included in the bulletins include SharePoint, Access, Exchange and .Net Framework.

There were 22 reported vulnerabilities affecting these services in 2014, with 4 classed as critical.

Conclusion

The figures from the 2014 Microsoft Vulnerabilities Report, largely reflect a significant uplift in the total number of vulnerabilities users are exposed to, with an increase of 63% in comparison to 2013. The report once again highlights how a significant number of Critical vulnerabilities could be mitigated by the removal of user admin rights, 97% in total.

These statistics serve as another reminder as to the importance of removing user admin rights in an enterprise setting. Analysts and respected industry bodies including SANS, The Council on Cyber Security and the Australian Department of Defense all list the controlled use of administrative privileges as a fundamental part of their security best practise guidelines.

Additionally, one of the most noticeable spikes in this year's research is a 99% year on year increase in the number of vulnerabilities affecting Internet Explorer, underlining why the internet is now one of the most common entry points for malware to find its way onto the network. Cyber criminals are becoming increasingly sophisticated and targeted in bypassing security controls, targeting individual users as a way to gain entry to corporate files and data.

One of the most effective ways to mitigate such threats is to remove administrator rights from users completely, using Privilege Management and Application Control technology to allow all users to function effectively under a standard user account. Complement

this by layering security strategies as part of a Defense in Depth (DiD) approach. The overlap of these layers of defense aim to ensure that the shortcomings of one security control are covered by another. For example, in the gap between a patch being discovered and applied, Sandboxing technology will trap and contain online threats so that data remains secure.

For more information on creating a layered approach to security, visit www.avecto.com/defendpoint

About Avecto

Avecto is a security software company that sees security as an enabler. We're all about finding technical solutions aligned with commercial benefits. We know, from experience, that technology has the power to facilitate transformational change.

Our proactive endpoint security software Defendpoint delivers on this promise by uniquely combining the technologies of Privilege Management, Application Control and Sandboxing. The benefits of the individual modules and our consultative methodology provides clients with a clearly mapped journey against measurable objectives to ensure project success.

And our focus on the end user means you can finally empower people to work freely without security compromise.

SC Magazine Awards 2013 Europe Winner

2013 Computing Security Awards Winner New Product of the Year

Deloitte. Technology Fast50 UK 2014

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 2014 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 is assigned a type from one of 7 categories;. Remote Code Execution, Elevation of Privilege, Information Disclosure, Denial of Service, Security Feature Bypass, Spoofing, Tampering– which occasionally vary depending on the individual piece 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.


Microsoft Security Bulletin MS14-080 - Critical

Cumulative Security Update for Internet Explorer (3008923)

Executive Summary

Affected Software

Figure 1: Example Microsoft Security Bulletin

Certain vulnerabilities have appeared in multiple bulletins throughout 2014, 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 generalisations 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.

Whilst 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 2014

Bulletin ID	Date	Vulnerability	Impact	Severity	Mitigated by Standard Rights
MS14-001	14/01/2014	CVE-2014-0258	Remote Code Execution	Important	Yes
MS14-001	14/01/2014	CVE-2014-0259	Remote Code Execution	Important	Yes
MS14-001	14/01/2014	CVE-2014-0260	Remote Code Execution	Important	Yes
MS14-002	14/01/2014	CVE-2013-5065	Elevation of Privilege	Important	No
MS14-003	14/01/2014	CVE-2014-0262	Elevation of Privilege	Important	No
MS14-004	14/01/2014	CVE-2014-0261	Denial of Service	Important	No
MS14-005	11/02/2014	CVE-2014-0266	Information Disclosure	Important	No
MS14-006	11/02/2014	CVE-2014-0254	Denial of Service	Important	No
MS14-007	28/02/2014	CVE-2014-0263	Remote Code Execution	Critical	Yes
MS14-008	11/02/2014	CVE-2014-0294	Remote Code Execution	Critical	No
MS14-009	11/02/2014	CVE-2014-0253	Denial of Service	Important	No
MS14-009	11/02/2014	CVE-2014-0257	Elevation of Privilege	Important	No
MS14-009	11/02/2014	CVE-2014-0295	Security Feature Bypass	Important	No
MS14-010	11/02/2014	CVE-2014-0267	Remote Code Execution	Critical	Yes
MS14-010	11/02/2014	CVE-2014-0268	Elevation of Privilege	Important	Yes
MS14-010	11/02/2014	CVE-2014-0269	Remote Code Execution	Critical	Yes
MS14-010	11/02/2014	CVE-2014-0270	Remote Code Execution	Critical	Yes
MS14-010	11/02/2014	CVE-2014-0272	Remote Code Execution	Critical	Yes
MS14-010	11/02/2014	CVE-2014-0273	Remote Code Execution	Critical	Yes
MS14-010	11/02/2014	CVE-2014-0274	Remote Code Execution	Critical	Yes
MS14-010	11/02/2014	CVE-2014-0275	Remote Code Execution	Critical	Yes
MS14-010	11/02/2014	CVE-2014-0276	Remote Code Execution	Critical	Yes
MS14-010	11/02/2014	CVE-2014-0277	Remote Code Execution	Critical	Yes
MS14-010	11/02/2014	CVE-2014-0278	Remote Code Execution	Critical	Yes
MS14-010	11/02/2014	CVE-2014-0279	Remote Code Execution	Critical	Yes
MS14-010	11/02/2014	CVE-2014-0280	Remote Code Execution	Critical	Yes

Bulletin ID	Date	Vulnerability	Impact	Severity	Mitigated by Standard Rights
MS14-010	11/02/2014	CVE-2014-0281	Remote Code Execution	Critical	Yes
MS14-010	11/02/2014	CVE-2014-0283	Remote Code Execution	Critical	Yes
MS14-010	11/02/2014	CVE-2014-0284	Remote Code Execution	Critical	Yes
MS14-010	11/02/2014	CVE-2014-0285	Remote Code Execution	Critical	Yes
MS14-010	11/02/2014	CVE-2014-0286	Remote Code Execution	Critical	Yes
MS14-010	11/02/2014	CVE-2014-0287	Remote Code Execution	Critical	Yes
MS14-010	11/02/2014	CVE-2014-0288	Remote Code Execution	Critical	Yes
MS14-010	11/02/2014	CVE-2014-0289	Remote Code Execution	Critical	Yes
MS14-010	11/02/2014	CVE-2014-0290	Remote Code Execution	Critical	Yes
MS14-010	11/02/2014	CVE-2014-0293	Information Disclosure	Important	Yes
MS14-011	11/02/2014	CVE-2014-0271	Remote Code Execution	Critical	No
MS14-012	11/03/2014	CVE-2014-0297	Remote Code Execution	Critical	Yes
MS14-012	11/03/2014	CVE-2014-0298	Remote Code Execution	Critical	Yes
MS14-012	11/03/2014	CVE-2014-0299	Remote Code Execution	Critical	Yes
MS14-012	11/03/2014	CVE-2014-0302	Remote Code Execution	Critical	Yes
MS14-012	11/03/2014	CVE-2014-0303	Remote Code Execution	Critical	Yes
MS14-012	11/03/2014	CVE-2014-0304	Remote Code Execution	Critical	Yes
MS14-012	11/03/2014	CVE-2014-0305	Remote Code Execution	Critical	Yes
MS14-012	11/03/2014	CVE-2014-0306	Remote Code Execution	Critical	Yes
MS14-012	11/03/2014	CVE-2014-0307	Remote Code Execution	Critical	Yes
MS14-012	11/03/2014	CVE-2014-0308	Remote Code Execution	Critical	Yes
MS14-012	11/03/2014	CVE-2014-0309	Remote Code Execution	Critical	Yes
MS14-012	11/03/2014	CVE-2014-0311	Remote Code Execution	Critical	Yes
MS14-012	11/03/2014	CVE-2014-0312	Remote Code Execution	Critical	Yes
MS14-012	11/03/2014	CVE-2014-0313	Remote Code Execution	Critical	Yes
MS14-012	11/03/2014	CVE-2014-0314	Remote Code Execution	Critical	Yes
MS14-012	11/03/2014	CVE-2014-0321	Remote Code Execution	Critical	Yes
MS14-012	11/03/2014	CVE-2014-0322	Remote Code Execution	Critical	Yes
MS14-012	11/03/2014	CVE-2014-0324	Remote Code Execution	Critical	Yes
MS14-013	11/03/2014	CVE-2014-0301	Remote Code Execution	Critical	Yes
MS14-014	11/03/2014	CVE-2014-0319	Security Feature Bypass	Important	Yes
MS14-015	11/03/2014	CVE-2014-0300	Elevation of Privilege	Important	No
MS14-015	11/03/2014	CVE-2014-0323	Information Disclosure	Important	No
MS14-016	11/03/2014	CVE-2014-0317	Security Feature Bypass	Important	No
MS14-017	08/04/2014	CVE-2014-1757	Remote Code Execution	Important	Yes
MS14-017	08/04/2014	CVE-2014-1758	Remote Code Execution	Important	Yes
MS14-017	08/04/2014	CVE-2014-1761	Remote Code Execution	Critical	Yes
MS14-018	08/04/2014	CVE-2014-0325	Remote Code Execution	Critical	Yes
MS14-018	08/04/2014	CVE-2014-1751	Remote Code Execution	Critical	Yes

Bulletin ID	Date	Vulnerability	Impact	Severity	Mitigated by Standard Rights
MS14-018	08/04/2014	CVE-2014-1752	Remote Code Execution	Critical	Yes
MS14-018	08/04/2014	CVE-2014-1753	Remote Code Execution	Critical	Yes
MS14-018	08/04/2014	CVE-2014-1755	Remote Code Execution	Critical	Yes
MS14-018	08/04/2014	CVE-2014-1760	Remote Code Execution	Critical	Yes
MS14-019	08/04/2014	CVE-2014-0315	Remote Code Execution	Critical	Yes
MS14-020	08/04/2014	CVE-2014-1759	Remote Code Execution	Important	Yes
MS14-021	01/05/2014	CVE-2014-1776	Remote Code Execution	Critical	Yes
MS14-022	13/05/2014	CVE-2014-0251	Remote Code Execution	Critical	No
MS14-022	13/05/2014	CVE-2014-1754	Elevation of Privilege	Important	No
MS14-022	13/05/2014	CVE-2014-1813	Remote Code Execution	Critical	No
MS14-023	13/05/2014	CVE-2014-1756	Remote Code Execution	Important	Yes
MS14-023	13/05/2014	CVE-2014-1808	Information Disclosure	Important	Yes
MS14-024	13/05/2014	CVE-2014-1809	Security Feature Bypass	Important	No
MS14-025	13/05/2014	CVE-2014-1812	Elevation of Privilege	Important	No
MS14-026	13/05/2014	CVE-2014-1806	Elevation of Privilege	Important	No
MS14-027	13/05/2014	CVE-2014-1807	Elevation of Privilege	Important	No
MS14-028	13/05/2014	CVE-2014-0255	Denial of Service	Important	No
MS14-028	13/05/2014	CVE-2014-0256	Denial of Service	Important	No
MS14-029	13/05/2014	CVE-2014-0310	Remote Code Execution	Critical	Yes
MS14-029	13/05/2014	CVE-2014-1815	Remote Code Execution	Critical	Yes
MS14-030	10/06/2014	CVE-2014-0296	Tampering	Important	No
MS14-031	10/06/2014	CVE-2014-1811	Denial of Service	Important	No
MS14-032	10/06/2014	CVE-2014-1823	Information Disclosure	Important	No
MS14-033	10/06/2014	CVE-2014-1816	Information Disclosure	Important	No
MS14-034	10/06/2014	CVE-2014-2778	Remote Code Execution	Important	Yes
MS14-035	10/06/2014	CVE-2014-0282	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1762	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1764	Elevation of Privilege	Important	Yes
MS14-035	10/06/2014	CVE-2014-1766	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1769	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1770	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1771	Information Disclosure	Important	Yes
MS14-035	10/06/2014	CVE-2014-1772	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1773	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1774	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1775	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1777	Information Disclosure	Important	Yes
MS14-035	10/06/2014	CVE-2014-1778	Elevation of Privilege	Important	Yes
MS14-035	10/06/2014	CVE-2014-1779	Remote Code Execution	Critical	Yes

Bulletin ID	Date	Vulnerability	Impact	Severity	Mitigated by Standard Rights
MS14-035	10/06/2014	CVE-2014-1780	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1781	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1782	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1783	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1784	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1785	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1786	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1788	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1789	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1790	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1791	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1792	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1794	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1795	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1796	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1797	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1799	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1800	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1802	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1803	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1804	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-1805	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-2753	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-2754	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-2755	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-2756	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-2757	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-2758	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-2759	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-2760	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-2761	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-2763	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-2764	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-2765	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-2766	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-2767	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-2768	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-2769	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-2770	Remote Code Execution	Critical	Yes

Bulletin ID	Date	Vulnerability	Impact	Severity	Mitigated by Standard Rights
MS14-035	10/06/2014	CVE-2014-2771	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-2772	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-2773	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-2775	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-2776	Remote Code Execution	Critical	Yes
MS14-035	10/06/2014	CVE-2014-2777	Elevation of Privilege	Important	Yes
MS14-035	10/06/2014	CVE-2014-2782	Remote Code Execution	Critical	Yes
MS14-036	10/06/2014	CVE-2014-1817	Remote Code Execution	Critical	Yes
MS14-036	10/06/2014	CVE-2014-1818	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-1763	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-1765	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-2783	Security Feature Bypass	Moderate	Yes
MS14-037	08/07/2014	CVE-2014-2785	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-2786	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-2787	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-2788	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-2789	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-2790	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-2791	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-2792	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-2794	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-2795	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-2797	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-2798	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-2800	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-2801	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-2802	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-2803	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-2804	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-2806	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-2807	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-2809	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-2813	Remote Code Execution	Critical	Yes
MS14-037	08/07/2014	CVE-2014-4066	Remote Code Execution	Critical	Yes
MS14-038	08/07/2014	CVE-2014-1824	Remote Code Execution	Critical	Yes
MS14-039	08/07/2014	CVE-2014-2781	Elevation of Privilege	Important	No
MS14-040	08/07/2014	CVE-2014-1767	Elevation of Privilege	Important	No
MS14-041	08/07/2014	CVE-2014-2780	Elevation of Privilege	Important	No
MS14-042	08/07/2014	CVE-2014-2814	Denial of Service	Moderate	No

Bulletin ID	Date	Vulnerability	Impact	Severity	Mitigated by Standard Rights
MS14-043	08/07/2014	CVE-2014-4060	Remote Code Execution	Critical	Yes
MS14-044	08/07/2014	CVE-2014-1820	Elevation of Privilege	Important	No
MS14-044	08/07/2014	CVE-2014-4061	Denial of Service	Important	No
MS14-045	08/07/2014	CVE-2014-0318	Elevation of Privilege	Important	No
MS14-045	08/07/2014	CVE-2014-1819	Elevation of Privilege	Important	No
MS14-045	08/07/2014	CVE-2014-4064	Information Disclosure	Important	No
MS14-046	08/07/2014	CVE-2014-4062	Security Feature Bypass	Important	No
MS14-047	08/07/2014	CVE-2014-0316	Security Feature Bypass	Important	No
MS14-048	08/07/2014	CVE-2014-2815	Remote Code Execution	Important	Yes
MS14-049	08/07/2014	CVE-2014-1814	Elevation of Privilege	Important	No
MS14-050	08/07/2014	CVE-2014-2816	Elevation of Privilege	Important	No
MS14-051	08/07/2014	CVE-2014-2774	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-2784	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-2796	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-2808	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-2810	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-2811	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-2817	Elevation of Privilege	Important	Yes
MS14-051	08/07/2014	CVE-2014-2818	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-2819	Elevation of Privilege	Important	Yes
MS14-051	08/07/2014	CVE-2014-2820	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-2821	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-2822	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-2823	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-2824	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-2825	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-2826	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-2827	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-4050	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-4051	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-4052	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-4055	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-4056	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-4057	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-4058	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-4063	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-4067	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-4145	Remote Code Execution	Critical	Yes
MS14-051	08/07/2014	CVE-2014-6354	Remote Code Execution	Critical	Yes

Bulletin ID	Date	Vulnerability	Impact	Severity	Mitigated by Standard Rights
MS14-052	09/09/2014	CVE-2013-7331	Information Disclosure	Important	Yes
MS14-052	09/09/2014	CVE-2014-2799	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4059	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4065	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4079	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4080	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4081	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4082	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4083	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4084	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4085	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4086	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4087	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4088	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4089	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4090	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4091	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4092	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4093	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4094	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4095	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4096	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4097	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4098	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4099	Denial of Service	Moderate	Yes
MS14-052	09/09/2014	CVE-2014-4100	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4101	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4102	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4103	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4104	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4105	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4106	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4107	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4108	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4109	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4110	Remote Code Execution	Critical	Yes
MS14-052	09/09/2014	CVE-2014-4111	Remote Code Execution	Critical	Yes
MS14-053	09/09/2014	CVE-2014-4072	Denial of Service	Important	No
MS14-054	09/09/2014	CVE-2014-4074	Elevation of Privilege	Important	No
MS14-055	09/09/2014	CVE-2014-4068	Denial of Service	Important	No

Bulletin ID	Date	Vulnerability	Impact	Severity	Mitigated by Standard Rights
MS14-055	09/09/2014	CVE-2014-4070	Information Disclosure	Important	No
MS14-055	09/09/2014	CVE-2014-4071	Denial of Service	Important	No
MS14-056	14/10/2014	CVE-2014-4123	Elevation of Privilege	Important	Yes
MS14-056	14/10/2014	CVE-2014-4124	Elevation of Privilege	Important	Yes
MS14-056	14/10/2014	CVE-2014-4126	Remote Code Execution	Critical	Yes
MS14-056	14/10/2014	CVE-2014-4127	Remote Code Execution	Critical	Yes
MS14-056	14/10/2014	CVE-2014-4128	Remote Code Execution	Critical	Yes
MS14-056	14/10/2014	CVE-2014-4129	Remote Code Execution	Critical	Yes
MS14-056	14/10/2014	CVE-2014-4130	Remote Code Execution	Critical	Yes
MS14-056	14/10/2014	CVE-2014-4132	Remote Code Execution	Critical	Yes
MS14-056	14/10/2014	CVE-2014-4133	Remote Code Execution	Critical	Yes
MS14-056	14/10/2014	CVE-2014-4134	Remote Code Execution	Critical	Yes
MS14-056	14/10/2014	CVE-2014-4137	Remote Code Execution	Critical	Yes
MS14-056	14/10/2014	CVE-2014-4138	Remote Code Execution	Critical	Yes
MS14-056	14/10/2014	CVE-2014-4140	Security Feature Bypass	Important	Yes
MS14-056	14/10/2014	CVE-2014-4141	Remote Code Execution	Critical	Yes
MS14-057	14/10/2014	CVE-2014-4073	Elevation of Privilege	Important	No
MS14-057	14/10/2014	CVE-2014-4121	Remote Code Execution	Critical	Yes
MS14-057	14/10/2014	CVE-2014-4122	Security Feature Bypass	Important	No
MS14-058	14/10/2014	CVE-2014-4113	Elevation of Privilege	Important	No
MS14-058	14/10/2014	CVE-2014-4148	Remote Code Execution	Critical	No
MS14-059	14/10/2014	CVE-2014-4075	Security Feature Bypass	Important	No
MS14-060	14/10/2014	CVE-2014-4114	Remote Code Execution	Important	Yes
MS14-061	14/10/2014	CVE-2014-4117	Remote Code Execution	Important	Yes
MS14-062	14/10/2014	CVE-2014-4971	Elevation of Privilege	Important	No
MS14-063	14/10/2014	CVE-2014-4115	Elevation of Privilege	Important	No
MS14-064	11/11/2014	CVE-2014-6332	Remote Code Execution	Critical	Yes
MS14-064	11/11/2014	CVE-2014-6352	Information Disclosure	Important	Yes
MS14-065	11/11/2014	CVE-2014-4143	Remote Code Execution	Critical	Yes
MS14-065	11/11/2014	CVE-2014-6323	Information Disclosure	Important	Yes
MS14-065	11/11/2014	CVE-2014-6337	Remote Code Execution	Critical	Yes
MS14-065	11/11/2014	CVE-2014-6339	Security Feature Bypass	Important	Yes
MS14-065	11/11/2014	CVE-2014-6340	Information Disclosure	Important	Yes
MS14-065	11/11/2014	CVE-2014-6341	Remote Code Execution	Critical	Yes
MS14-065	11/11/2014	CVE-2014-6342	Remote Code Execution	Critical	Yes
MS14-065	11/11/2014	CVE-2014-6343	Remote Code Execution	Critical	Yes
MS14-065	11/11/2014	CVE-2014-6344	Remote Code Execution	Critical	Yes
MS14-065	11/11/2014	CVE-2014-6345	Information Disclosure	Important	Yes
MS14-065	11/11/2014	CVE-2014-6346	Information Disclosure	Important	Yes

Bulletin ID	Date	Vulnerability	Impact	Severity	Mitigated by Standard Rights
MS14-065	11/11/2014	CVE-2014-6347	Remote Code Execution	Critical	Yes
MS14-065	11/11/2014	CVE-2014-6348	Remote Code Execution	Critical	Yes
MS14-065	11/11/2014	CVE-2014-6349	Elevation of Privilege	Important	Yes
MS14-065	11/11/2014	CVE-2014-6350	Elevation of Privilege	Important	Yes
MS14-065	11/11/2014	CVE-2014-6351	Remote Code Execution	Critical	Yes
MS14-065	11/11/2014	CVE-2014-6353	Remote Code Execution	Critical	Yes
MS14-066	11/11/2014	CVE-2014-6321	Remote Code Execution	Critical	No
MS14-067	11/11/2014	CVE-2014-4118	Remote Code Execution	Critical	Yes
MS14-068	18/11/2014	CVE-2014-6324	Elevation of Privilege	Critical	No
MS14-069	11/11/2014	CVE-2014-6333	Remote Code Execution	Important	Yes
MS14-069	11/11/2014	CVE-2014-6334	Remote Code Execution	Important	Yes
MS14-069	11/11/2014	CVE-2014-6335	Remote Code Execution	Important	Yes
MS14-070	11/11/2014	CVE-2014-4076	Elevation of Privilege	Important	No
MS14-071	11/11/2014	CVE-2014-6322	Elevation of Privilege	Important	No
MS14-072	11/11/2014	CVE-2014-4149	Elevation of Privilege	Important	No
MS14-073	11/11/2014	CVE-2014-4116	Elevation of Privilege	Important	No
MS14-074	11/11/2014	CVE-2014-6318	Security Feature Bypass	Important	No
MS14-075	09/12/2014	CVE-2014-6319	Spoofing	Important	No
MS14-075	09/12/2014	CVE-2014-6325	Elevation of Privilege	Important	No
MS14-075	09/12/2014	CVE-2014-6326	Elevation of Privilege	Important	No
MS14-075	09/12/2014	CVE-2014-6336	Spoofing	Important	No
MS14-076	11/11/2014	CVE-2014-4078	Security Feature Bypass	Important	No
MS14-077	11/11/2014	CVE-2014-6331	Information Disclosure	Important	No
MS14-078	11/11/2014	CVE-2014-4077	Elevation of Privilege	Moderate	No
MS14-079	11/11/2014	CVE-2014-6317	Denial of Service	Moderate	No
MS14-080	09/12/2014	CVE-2014-6327	Remote Code Execution	Critical	Yes
MS14-080	09/12/2014	CVE-2014-6328	Security Feature Bypass	Important	Yes
MS14-080	09/12/2014	CVE-2014-6329	Remote Code Execution	Critical	Yes
MS14-080	09/12/2014	CVE-2014-6330	Remote Code Execution	Critical	Yes
MS14-080	09/12/2014	CVE-2014-6365	Security Feature Bypass	Important	Yes
MS14-080	09/12/2014	CVE-2014-6366	Remote Code Execution	Critical	Yes
MS14-080	09/12/2014	CVE-2014-6368	Security Feature Bypass	Important	Yes
MS14-080	09/12/2014	CVE-2014-6369	Remote Code Execution	Critical	Yes
MS14-080	09/12/2014	CVE-2014-6373	Remote Code Execution	Critical	Yes
MS14-080	09/12/2014	CVE-2014-6374	Remote Code Execution	Critical	Yes
MS14-080	09/12/2014	CVE-2014-6375	Remote Code Execution	Critical	Yes
MS14-080	09/12/2014	CVE-2014-6376	Remote Code Execution	Critical	Yes
MS14-080	09/12/2014	CVE-2014-8966	Remote Code Execution	Critical	Yes
MS14-081	09/12/2014	CVE-2014-6356	Remote Code Execution	Critical	Yes

Bulletin ID	Date	Vulnerability	Impact	Severity	Mitigated by Standard Rights
MS14-081	09/12/2014	CVE-2014-6357	Remote Code Execution	Critical	Yes
MS14-082	09/12/2014	CVE-2014-6364	Remote Code Execution	Important	Yes
MS14-083	09/12/2014	CVE-2014-6360	Remote Code Execution	Important	Yes
MS14-083	09/12/2014	CVE-2014-6361	Remote Code Execution	Important	Yes
MS14-084	09/12/2014	CVE-2014-6363	Remote Code Execution	Critical	No
MS14-085	09/12/2014	CVE-2014-6355	Information Disclosure	Important	No