



2015 Microsoft Vulnerabilities Study: Mitigating risk by removing user privileges

Analysis of Microsoft “Patch Tuesday” Security Bulletins from 2015 highlights that 85% of Critical Microsoft vulnerabilities would be mitigated by removing admin rights across an enterprise, with a 52% increase in the total volume of vulnerabilities compared to 2014.





Contents

| | |
|---|----|
| Introduction | 2 |
| Methodology | 2 |
| Key findings | 3 |
| Vulnerability Categories | 4 |
| Microsoft Windows vulnerabilites | 5 |
| Internet Explorer | 6 |
| Microsoft Office | 7 |
| Windows Servers | 8 |
| Additional Microsoft services | 9 |
| Conclusion | 9 |
| About Avecto | 11 |
| Appendix | 12 |



Introduction

Compiled by Avecto, this report analyzes the data from security bulletins issued by Microsoft throughout 2015. 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 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.

In 2015, it was widely reported that Microsoft’s Patch Tuesday approach would change for all Windows 10 devices, with an approach of patches being released as soon as they are available. This effectively increases response time by as much as a month, cutting down the time between a vulnerability being discovered (Zero Day) and the patch being rolled and applied.

The 2015 Microsoft Vulnerabilities Report is the third iteration of Avecto’s research. In 2014, the same report found a total of 240 vulnerabilities with a Critical rating. This year’s report reveals 251 Critical vulnerabilities; an increase of around 5% year on year and 71% increase on the 2013 study.

The overall number of vulnerabilities has risen significantly in this period, from 345 to 524, representing an annual increase of 52%.

The report finds that the risk associated with 85% of Critical vulnerabilities could be mitigated by removing 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.

*Some started with “Customers” rather than “users”.



Key findings

The 2015 report highlights the following key findings:

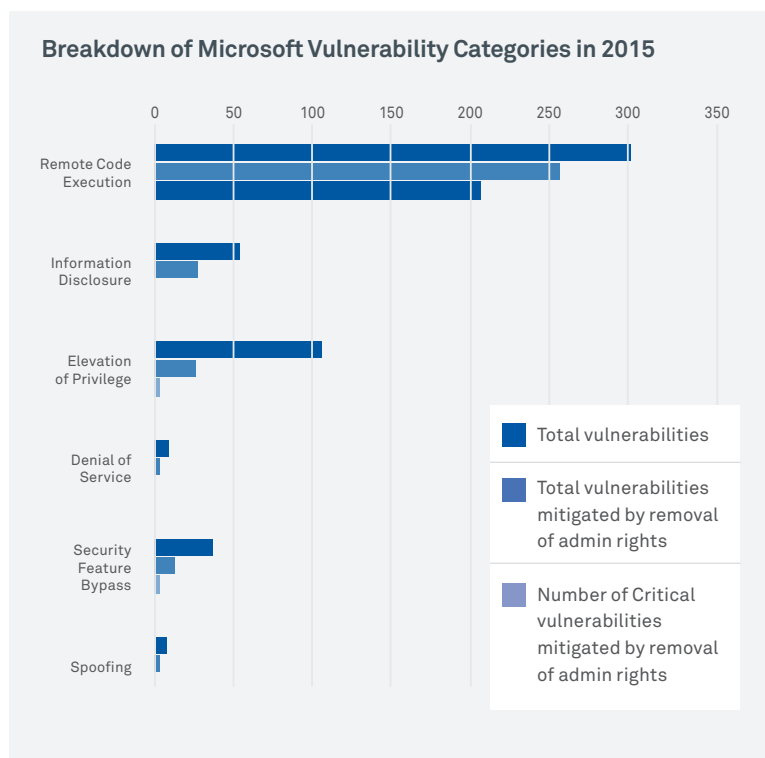
- > Of the 251 vulnerabilities in 2015 with a Critical rating, 85% were concluded to be mitigated by removing administrator rights
- > There has been a 52% year on year rise in the volume of vulnerabilities since 2014
- > 86% of Critical vulnerabilities affecting Windows could be mitigated by removing admin rights
- > 99.5% of all vulnerabilities in Internet Explorer could be mitigated by removing admin rights
- > 82% of vulnerabilities affecting Microsoft Office could be mitigated by removing admin rights
- > 85% of Remote Code Execution vulnerabilities could be mitigated by removing admin rights
- > 82% Critical vulnerabilities affecting Windows 10 could be mitigated by removing admin rights
- > 63% of all **Microsoft vulnerabilities** reported in 2015 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 2015 were categorised 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 once again account for the largest proportion of total Microsoft vulnerabilities, increasing by 15% compared to 2014. Of these, **82% were classed as Critical** and **85% of these updates could be mitigated by removal of admin rights**.

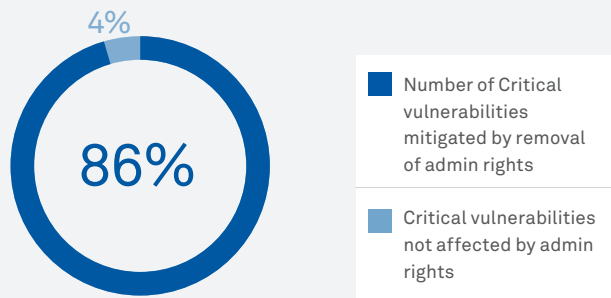




Microsoft Windows vulnerabilities

In 2015, 433 vulnerabilities were reported across Windows Vista, Windows 7, Windows RT, Windows 8 / 8.1 and Windows 10 operating systems compared to 300 in 2014.

Critical Windows vulnerabilities mitigated by removal of admin rights in 2015



86% of Critical vulnerabilities affecting Microsoft Windows in 2015 could be mitigated by the removal of admin rights.

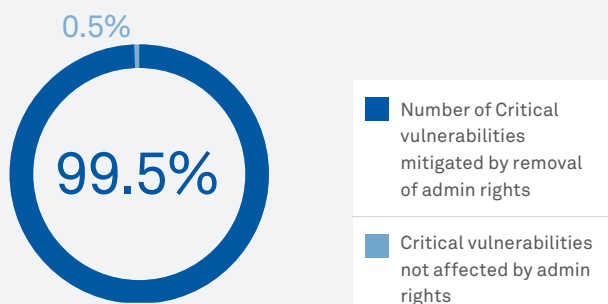


Internet Explorer

In 2015, a total of 238 vulnerabilities were reported that affected Internet Explorer (IE) versions 6 - 11. The volume has fallen slightly compared to 2014 (245) but has jumped from 123 in 2013. 99.5% of IE vulnerabilities in 2015 could be mitigated by the removal of user admin rights.

Notably, 100% of the vulnerabilities reported in Edge (29) would be mitigated by removing admin rights.

Internet Explorer vulnerabilities Mitigated by Removal of Admin Rights in 2015





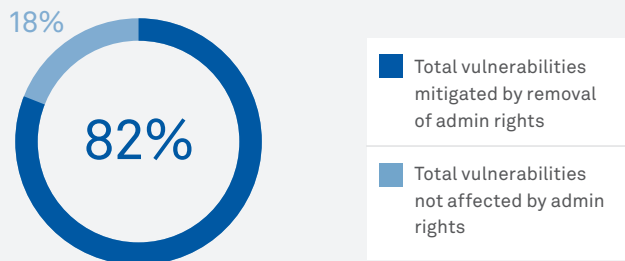
Microsoft Office

In 2015, 62 vulnerabilities were published in Microsoft Security Bulletins affecting Microsoft Office products, compared to just 20 in 2014, an increase of 210%.

This encompasses, Office 2010, Office 2013, Office 2016, Microsoft Excel, Word, PowerPoint, Visio and Publisher amongst others. Removing admin rights would mitigate 82% of these Office vulnerabilities.

Notably, 100% of those vulnerabilities in Office 2016, the latest version of Microsoft's software, could have been mitigated by admin rights removal.

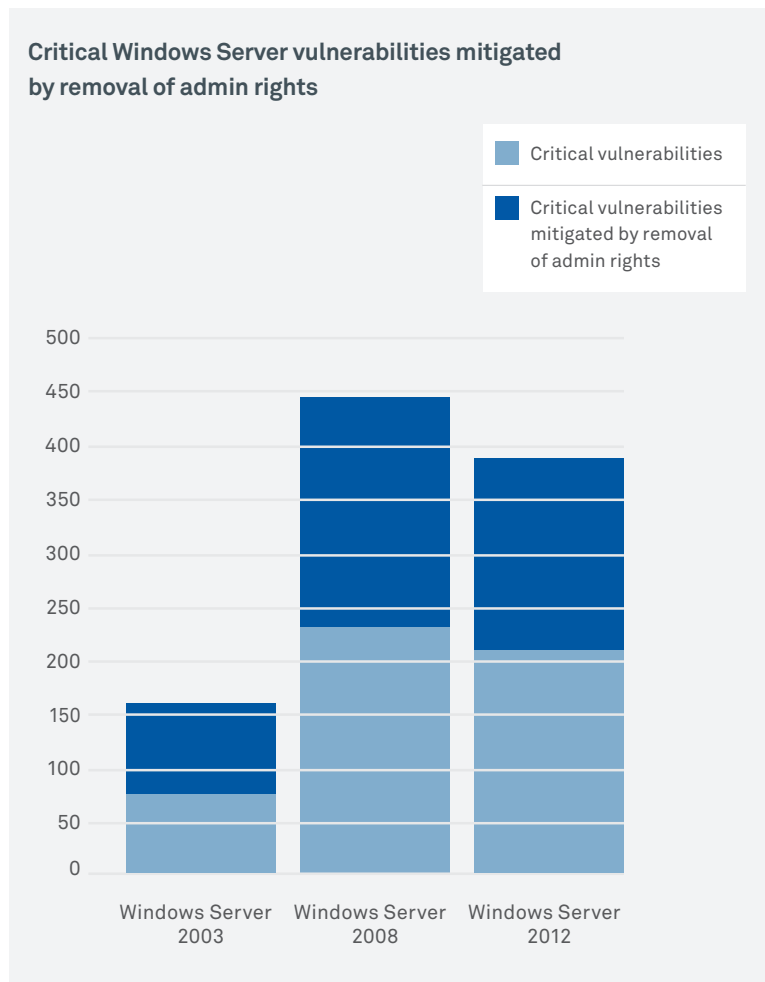
Total Windows Office Vulnerabilities in 2015





Windows Server vulnerabilities

429 vulnerabilities were reported in Microsoft Security Bulletins affecting Microsoft Windows Server in 2015, compared to 304 in 2014. Of the 240 vulnerabilities with a Critical rating in 2015, 85% were found to be mitigated by the removal of admin rights.





Additional Microsoft Services

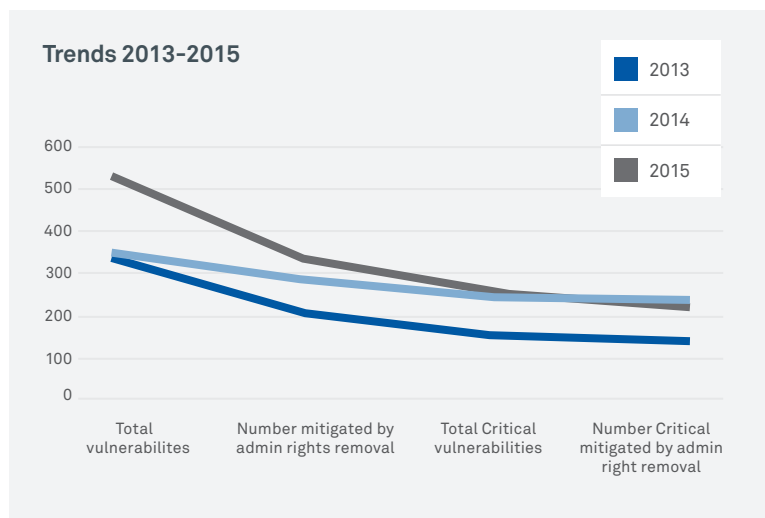
There were 18 reported vulnerabilities affecting the .Net Framework, up from 10 in 2014. 28% of these vulnerabilities would be mitigated by removing admin rights.

Conclusion

The figures from the 2015 Microsoft Vulnerabilities Study once again highlights a significant uplift in the total number of vulnerabilities users are exposed to, rising 52% year on year.

“ Users should never log in as administrator and never have administrator rights for their systems. ”

Dr Eric Cole, SANS Institute



While the percentage of vulnerabilities mitigated by removing admin rights has fallen, the overall number of vulnerabilities has increased significantly, highlighting the pervasive and growing threats faced by the enterprise.

Attackers are becoming increasingly intelligent, with unique and targeted attacks that often evade detection. In 60% of cases, attackers are able to compromise an organization within minutes (Verizon DBIR 2015.)



Avecto recommends following the security best practises advocated by industry experts including SANS, The Council on Cyber Security and the Australian Department of Defense. The consistent advice is to minimize risk by implementing application whitelisting, patch the operating system and software and adopt an approach of least privilege.

*<http://searchsecurity.techtarget.com/tip/Six-ways-to-improve-endpoint-device-security>



About Avecto

Avecto is a global software company specializing in endpoint security. Its unique Defendpoint software makes prevention possible, integrating three proactive technologies to stop malware at the endpoint. This innovative software protects over 5 million endpoints across the world's most recognizable brands. Avecto promotes a balance of security + freedom, focusing on a positive user experience across every software implementation.

About Defendpoint

Defendpoint by Avecto is a security software solution that makes prevention possible. For the first time, it uniquely integrates three proactive technologies to stop malware at the endpoint.

The combination of Privilege Management, Application Control and Sandboxing in a single suite solution finally allows global organizations to improve security while ensuring a positive user experience across Windows and OS X.

It allows you to create a solid security foundation by removing admin rights from all users while empowering them to perform their day to day job roles by instead assigning privileges directly to applications, tasks, scripts and content.

With pragmatic application whitelisting rules, known and trusted applications are elevated automatically, while untrusted applications are blocked with comprehensive options for managing exceptions. Sandboxing adds a final layer of defense, isolating the web browser and downloaded content to contain any threats that originate online.

When traditional security solutions such as antivirus are only effective half of the time, Defendpoint takes a proactive approach to defending the endpoint.



UK

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

Phone 0845 519 0114
Fax 0845 519 0115

USA

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

Germany

D-61348 Bad Homburg
Merkurhaus Bad Homburg,
Hessening 121/119

Phone 0845 519 0114
Fax 0845 519 0115



Appendix 1: Detailed Methodology

Data source

This report has been compiled following analysis of the Security bulletins published in 2015 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 MS15-135 – Important
Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege Vulnerability
 Published: December 8, 2015
 Version: 1.0

Executive Summary
 This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker is able to execute code on a system and runs a specially crafted application.
 This security update is rated Important for supported releases of Microsoft Windows. For more information, see the **Affected Software** section.
 The update addresses the vulnerability by correcting how the Windows kernel and Windows font drivers handle objects in memory. For more information about the vulnerability, see the **Vulnerability Information** section.
 For more information about this update, see Microsoft Knowledge Base Article 3119075.

Affected Software and Vulnerability Severity Ratings
 The following software versions or editions are affected. Versions or editions that are not listed are either past their support life cycle or do not have a support life cycle. To determine the support life cycle for your software version or edition, see Microsoft Support Lifecycle.
 The severity ratings indicated for each affected software assume the potential maximum impact of the vulnerability. For information on the severity ratings, the exploitability of the vulnerability in relation to its severity rating and security impact, please see the **Exploitability** section.

| Vulnerability Severity Rating and Maximum Security Impact by Affected Software | | | | |
|--|--|--|--|--|
| Operating System | Windows Kernel Memory Elevation of Privilege Vulnerability - CVE-2015-617* | Windows Kernel Memory Elevation of Privilege Vulnerability - CVE-2015-617* | Windows Kernel Memory Elevation of Privilege Vulnerability - CVE-2015-617* | Windows Elevation of Privilege Vulnerability - CVE-2015-617* |
| | | | | |

Figure 1: Example Microsoft Security Bulletin



Certain vulnerabilities have appeared in multiple bulletins throughout 2015, 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 11 and for Windows 7” is taken as a vulnerability for **Internet Explorer 11 and Windows 7**.



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 2015

| Bulletin | Vulnerability | Severity Rating | Impact | Mitigated |
|--------------------------|---------------|-----------------|-------------------------|-----------|
| MS15-001 | CVE-2015-0002 | Important | Elevation of Privilege | No |
| MS15-002 | CVE-2015-0014 | Critical | Remote Code Execution | No |
| MS15-003 | CVE-2015-0004 | Important | Elevation of Privilege | No |
| MS15-004 | CVE-2015-0016 | Important | Elevation of Privilege | Yes |
| MS15-005 | CVE-2015-0006 | Important | Security Feature Bypass | No |
| MS15-006 | CVE-2015-0001 | Important | Security Feature Bypass | Yes |
| MS15-007 | CVE-2015-0015 | Important | Denial of Service | No |
| MS15-008 | CVE-2015-0011 | Important | Elevation of Privilege | No |
| MS15-009 | CVE-2014-8967 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0017 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0018 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0019 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0020 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0021 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0022 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0023 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0025 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0026 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0027 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0028 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0029 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0030 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0031 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0035 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0036 | Critical | Remote Code Execution | Yes |



| Bulletin | Vulnerability | Severity Rating | Impact | Mitigated |
|----------|---------------|-----------------|-------------------------|-----------|
| MS15-009 | CVE-2015-0037 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0038 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0039 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0040 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0041 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0042 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0043 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0044 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0045 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0046 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0048 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0049 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0050 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0051 | Important | Security Feature Bypass | Yes |
| MS15-009 | CVE-2015-0052 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0053 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0054 | Important | Elevation of Privilege | Yes |
| MS15-009 | CVE-2015-0055 | Critical | Elevation of Privilege | Yes |
| MS15-009 | CVE-2015-0066 | Critical | Elevation of Privilege | Yes |
| MS15-009 | CVE-2015-0067 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0068 | Critical | Remote Code Execution | Yes |
| MS15-009 | CVE-2015-0069 | Important | Information Disclosure | Yes |
| MS15-009 | CVE-2015-0070 | Important | Information Disclosure | Yes |
| MS15-009 | CVE-2015-0071 | Critical | Security Feature Bypass | Yes |
| MS15-010 | CVE-2015-0003 | Important | Denial of Service | No |
| MS15-010 | CVE-2015-0010 | Important | Security Feature Bypass | No |
| MS15-010 | CVE-2015-0057 | Important | Elevation of Privilege | No |
| MS15-010 | CVE-2015-0058 | Important | Elevation of Privilege | No |
| MS15-010 | CVE-2015-0059 | Critical | Remote Code Execution | No |
| MS15-010 | CVE-2015-0060 | Moderate | Denial of Service | No |
| MS15-011 | CVE-2015-0008 | Critical | Remote Code Execution | No |
| MS15-012 | CVE-2015-0063 | Important | Remote Code Execution | Yes |
| MS15-012 | CVE-2015-0064 | Important | Remote Code Execution | Yes |
| MS15-012 | CVE-2015-0065 | Important | Remote Code Execution | Yes |
| MS15-013 | CVE-2014-6362 | Important | Security Feature Bypass | No |
| MS15-014 | CVE-2015-0009 | Important | Security Feature Bypass | No |
| MS15-015 | CVE-2015-0062 | Important | Elevation of Privilege | No |
| MS15-016 | CVE-2015-0061 | Important | Information Disclosure | No |
| MS15-017 | CVE-2015-0012 | Important | Elevation of Privilege | No |



| Bulletin | Vulnerability | Severity Rating | Impact | Mitigated |
|----------|---------------|-----------------|------------------------|-----------|
| MS15-018 | CVE-2015-0056 | Critical | Remote Code Execution | Yes |
| MS15-018 | CVE-2015-0072 | Critical | Remote Code Execution | Yes |
| MS15-018 | CVE-2015-0099 | Critical | Remote Code Execution | Yes |
| MS15-018 | CVE-2015-0100 | Critical | Remote Code Execution | Yes |
| MS15-018 | CVE-2015-1622 | Critical | Remote Code Execution | Yes |
| MS15-018 | CVE-2015-1623 | Critical | Remote Code Execution | Yes |
| MS15-018 | CVE-2015-1624 | Critical | Remote Code Execution | Yes |
| MS15-018 | CVE-2015-1625 | Critical | Remote Code Execution | Yes |
| MS15-018 | CVE-2015-1626 | Critical | Remote Code Execution | Yes |
| MS15-018 | CVE-2015-1627 | Critical | Remote Code Execution | Yes |
| MS15-018 | CVE-2015-1634 | Critical | Remote Code Execution | Yes |
| MS15-019 | CVE-2015-0032 | Critical | Remote Code Execution | Yes |
| MS15-020 | CVE-2015-0081 | Critical | Remote Code Execution | No |
| MS15-020 | CVE-2015-0096 | Critical | Remote Code Execution | Yes |
| MS15-021 | CVE-2015-0074 | Moderate | Denial of Service | No |
| MS15-021 | CVE-2015-0087 | Important | Information Disclosure | No |
| MS15-021 | CVE-2015-0088 | Critical | Remote Code Execution | No |
| MS15-021 | CVE-2015-0089 | Important | Information Disclosure | No |
| MS15-021 | CVE-2015-0090 | Critical | Remote Code Execution | No |
| MS15-021 | CVE-2015-0091 | Critical | Remote Code Execution | No |
| MS15-021 | CVE-2015-0092 | Critical | Remote Code Execution | No |
| MS15-021 | CVE-2015-0093 | Critical | Remote Code Execution | No |
| MS15-022 | CVE-2015-0085 | Important | Remote Code Execution | Yes |
| MS15-022 | CVE-2015-0086 | Critical | Remote Code Execution | Yes |
| MS15-022 | CVE-2015-0097 | Important | Remote Code Execution | Yes |
| MS15-022 | CVE-2015-1633 | Important | Elevation of Privilege | Yes |
| MS15-022 | CVE-2015-1636 | Important | Elevation of Privilege | Yes |
| MS15-023 | CVE-2015-0077 | Important | Information Disclosure | No |
| MS15-023 | CVE-2015-0078 | Important | Elevation of Privilege | No |
| MS15-023 | CVE-2015-0094 | Important | Information Disclosure | No |
| MS15-023 | CVE-2015-0095 | Important | Information Disclosure | No |
| MS15-024 | CVE-2015-0080 | Important | Information Disclosure | No |
| MS15-025 | CVE-2015-0073 | Important | Elevation of Privilege | No |
| MS15-025 | CVE-2015-0075 | Important | Elevation of Privilege | No |
| MS15-026 | CVE-2015-1628 | Important | Elevation of Privilege | No |
| MS15-026 | CVE-2015-1629 | Important | Elevation of Privilege | No |
| MS15-026 | CVE-2015-1630 | Important | Elevation of Privilege | No |
| MS15-026 | CVE-2015-1631 | Important | Spoofing | No |
| MS15-026 | CVE-2015-1632 | Important | Elevation of Privilege | No |



| Bulletin | Vulnerability | Severity Rating | Impact | Mitigated |
|----------|---------------|-----------------|-------------------------|-----------|
| MS15-027 | CVE-2015-0005 | Important | Spoofing | No |
| MS15-028 | CVE-2015-0084 | Important | Security Feature Bypass | No |
| MS15-029 | CVE-2015-0076 | Important | Information Disclosure | No |
| MS15-030 | CVE-2015-0079 | Important | Denial of Service | No |
| MS15-031 | CVE-2015-1637 | Important | Security Feature Bypass | No |
| MS15-032 | CVE-2015-1652 | Critical | Remote Code Execution | Yes |
| MS15-032 | CVE-2015-1657 | Critical | Remote Code Execution | Yes |
| MS15-032 | CVE-2015-1659 | Critical | Remote Code Execution | Yes |
| MS15-032 | CVE-2015-1660 | Critical | Remote Code Execution | Yes |
| MS15-032 | CVE-2015-1661 | Important | Security Feature Bypass | Yes |
| MS15-032 | CVE-2015-1662 | Critical | Remote Code Execution | Yes |
| MS15-032 | CVE-2015-1665 | Critical | Remote Code Execution | Yes |
| MS15-032 | CVE-2015-1666 | Critical | Remote Code Execution | Yes |
| MS15-032 | CVE-2015-1667 | Critical | Remote Code Execution | Yes |
| MS15-032 | CVE-2015-1668 | Critical | Remote Code Execution | Yes |
| MS15-033 | CVE-2015-1641 | Important | Remote Code Execution | Yes |
| MS15-033 | CVE-2015-1649 | Critical | Remote Code Execution | Yes |
| MS15-033 | CVE-2015-1650 | Important | Remote Code Execution | Yes |
| MS15-033 | CVE-2015-1651 | Critical | Remote Code Execution | Yes |
| MS15-033 | CVE-2015-1639 | Important | Elevation of Privilege | Yes |
| MS15-034 | CVE-2015-1635 | Critical | Remote Code Execution | No |
| MS15-035 | CVE-2015-1645 | Critical | Remote Code Execution | Yes |
| MS15-036 | CVE-2015-1640 | Important | Elevation of Privilege | No |
| MS15-036 | CVE-2015-1653 | Important | Elevation of Privilege | No |
| MS15-037 | CVE-2015-0098 | Important | Elevation of Privilege | No |
| MS15-038 | CVE-2015-1643 | Important | Elevation of Privilege | No |
| MS15-038 | CVE-2015-1644 | Important | Elevation of Privilege | No |
| MS15-039 | CVE-2015-1646 | Important | Security Feature Bypass | No |
| MS15-040 | CVE-2015-1638 | Important | Information Disclosure | No |
| MS15-041 | CVE-2015-1648 | Important | Information Disclosure | No |
| MS15-042 | CVE-2015-1647 | Important | Denial of Service | No |
| MS15-043 | CVE-2015-1658 | Critical | Remote Code Execution | Yes |
| MS15-043 | CVE-2015-1685 | Important | Security Feature Bypass | Yes |
| MS15-043 | CVE-2015-1688 | Important | Elevation of Privilege | Yes |
| MS15-043 | CVE-2015-1689 | Critical | Remote Code Execution | Yes |
| MS15-043 | CVE-2015-1691 | Critical | Remote Code Execution | Yes |
| MS15-043 | CVE-2015-1692 | Important | Information Disclosure | Yes |
| MS15-043 | CVE-2015-1694 | Critical | Remote Code Execution | Yes |
| MS15-043 | CVE-2015-1703 | Important | Elevation of Privilege | Yes |



| Bulletin | Vulnerability | Severity Rating | Impact | Mitigated |
|--------------------------|---------------|-----------------|-------------------------|-----------|
| MS15-043 | CVE-2015-1704 | Important | Elevation of Privilege | Yes |
| MS15-043 | CVE-2015-1705 | Critical | Remote Code Execution | Yes |
| MS15-043 | CVE-2015-1706 | Critical | Remote Code Execution | Yes |
| MS15-043 | CVE-2015-1708 | Critical | Remote Code Execution | Yes |
| MS15-043 | CVE-2015-1709 | Critical | Remote Code Execution | Yes |
| MS15-043 | CVE-2015-1710 | Critical | Remote Code Execution | Yes |
| MS15-043 | CVE-2015-1711 | Critical | Remote Code Execution | Yes |
| MS15-043 | CVE-2015-1712 | Critical | Remote Code Execution | Yes |
| MS15-043 | CVE-2015-1713 | Important | Elevation of Privilege | Yes |
| MS15-043 | CVE-2015-1714 | Critical | Remote Code Execution | Yes |
| MS15-043 | CVE-2015-1717 | Critical | Remote Code Execution | Yes |
| MS15-043 | CVE-2015-1718 | Critical | Remote Code Execution | Yes |
| MS15-044 | CVE-2015-1670 | Important | Information Disclosure | No |
| MS15-044 | CVE-2015-1671 | Critical | Remote Code Execution | No |
| MS15-045 | CVE-2015-1675 | Critical | Remote Code Execution | Yes |
| MS15-045 | CVE-2015-1695 | Critical | Remote Code Execution | Yes |
| MS15-045 | CVE-2015-1696 | Critical | Remote Code Execution | Yes |
| MS15-045 | CVE-2015-1697 | Critical | Remote Code Execution | Yes |
| MS15-045 | CVE-2015-1698 | Critical | Remote Code Execution | Yes |
| MS15-045 | CVE-2015-1699 | Critical | Remote Code Execution | Yes |
| MS15-046 | CVE-2015-1682 | Important | Remote Code Execution | Yes |
| MS15-046 | CVE-2015-1683 | Important | Remote Code Execution | Yes |
| MS15-047 | CVE-2015-1700 | Important | Remote Code Execution | No |
| MS15-048 | CVE-2015-1672 | Important | Denial of Service | No |
| MS15-048 | CVE-2015-1673 | Important | Elevation of Privilege | Yes |
| MS15-049 | CVE-2015-1715 | Important | Elevation of Privilege | No |
| MS15-050 | CVE-2015-1702 | Important | Elevation of Privilege | No |
| MS15-051 | CVE-2015-1676 | Important | Information Disclosure | No |
| MS15-051 | CVE-2015-1677 | Important | Information Disclosure | No |
| MS15-051 | CVE-2015-1678 | Important | Information Disclosure | No |
| MS15-051 | CVE-2015-1679 | Important | Information Disclosure | No |
| MS15-051 | CVE-2015-1680 | Important | Information Disclosure | No |
| MS15-051 | CVE-2015-1701 | Important | Elevation of Privilege | No |
| MS15-052 | CVE-2015-1674 | Important | Security Feature Bypass | No |
| MS15-053 | CVE-2015-1684 | Important | Security Feature Bypass | Yes |
| MS15-053 | CVE-2015-1686 | Important | Security Feature Bypass | Yes |
| MS15-054 | CVE-2015-1681 | Important | Denial of Service | No |
| MS15-055 | CVE-2015-1716 | Important | Information Disclosure | No |
| MS15-056 | CVE-2015-1687 | Critical | Remote Code Execution | Yes |



| Bulletin | Vulnerability | Severity Rating | Impact | Mitigated |
|--------------------------|---------------|-----------------|------------------------|-----------|
| MS15-056 | CVE-2015-1730 | Critical | Remote Code Execution | Yes |
| MS15-056 | CVE-2015-1731 | Critical | Remote Code Execution | Yes |
| MS15-056 | CVE-2015-1732 | Critical | Remote Code Execution | Yes |
| MS15-056 | CVE-2015-1735 | Critical | Remote Code Execution | Yes |
| MS15-056 | CVE-2015-1736 | Critical | Remote Code Execution | Yes |
| MS15-056 | CVE-2015-1737 | Critical | Remote Code Execution | Yes |
| MS15-056 | CVE-2015-1739 | Important | Elevation of Privilege | Yes |
| MS15-056 | CVE-2015-1740 | Critical | Remote Code Execution | Yes |
| MS15-056 | CVE-2015-1741 | Critical | Remote Code Execution | Yes |
| MS15-056 | CVE-2015-1742 | Critical | Remote Code Execution | Yes |
| MS15-056 | CVE-2015-1743 | Important | Elevation of Privilege | Yes |
| MS15-056 | CVE-2015-1744 | Critical | Remote Code Execution | Yes |
| MS15-056 | CVE-2015-1745 | Critical | Remote Code Execution | Yes |
| MS15-056 | CVE-2015-1747 | Critical | Remote Code Execution | Yes |
| MS15-056 | CVE-2015-1748 | Important | Elevation of Privilege | Yes |
| MS15-056 | CVE-2015-1750 | Critical | Remote Code Execution | Yes |
| MS15-056 | CVE-2015-1751 | Critical | Remote Code Execution | Yes |
| MS15-056 | CVE-2015-1752 | Critical | Remote Code Execution | Yes |
| MS15-056 | CVE-2015-1753 | Critical | Remote Code Execution | Yes |
| MS15-056 | CVE-2015-1754 | Critical | Remote Code Execution | Yes |
| MS15-056 | CVE-2015-1755 | Critical | Remote Code Execution | Yes |
| MS15-056 | CVE-2015-1765 | Important | Information Disclosure | Yes |
| MS15-056 | CVE-2015-1766 | Critical | Remote Code Execution | Yes |
| MS15-057 | CVE-2015-1728 | Critical | Remote Code Execution | Yes |
| MS15-058 | CVE-2015-1761 | Important | Elevation of Privilege | No |
| MS15-058 | CVE-2015-1762 | Important | Remote Code Execution | No |
| MS15-058 | CVE-2015-1763 | Important | Remote Code Execution | No |
| MS15-059 | CVE-2015-1759 | Important | Remote Code Execution | Yes |
| MS15-059 | CVE-2015-1760 | Important | Remote Code Execution | Yes |
| MS15-059 | CVE-2015-1770 | Important | Remote Code Execution | Yes |
| MS15-060 | CVE-2015-1756 | Important | Remote Code Execution | No |
| MS15-061 | CVE-2015-1719 | Important | Information Disclosure | No |
| MS15-061 | CVE-2015-1720 | Important | Elevation of Privilege | No |
| MS15-061 | CVE-2015-1721 | Important | Elevation of Privilege | No |
| MS15-061 | CVE-2015-1722 | Important | Elevation of Privilege | No |
| MS15-061 | CVE-2015-1723 | Important | Elevation of Privilege | No |
| MS15-061 | CVE-2015-1724 | Important | Elevation of Privilege | No |
| MS15-061 | CVE-2015-1725 | Important | Elevation of Privilege | No |
| MS15-061 | CVE-2015-1726 | Important | Elevation of Privilege | No |



| Bulletin | Vulnerability | Severity Rating | Impact | Mitigated |
|----------|---------------|-----------------|-------------------------|-----------|
| MS15-061 | CVE-2015-1727 | Important | Elevation of Privilege | No |
| MS15-061 | CVE-2015-1768 | Important | Elevation of Privilege | No |
| MS15-061 | CVE-2015-2360 | Important | Elevation of Privilege | No |
| MS15-062 | CVE-2015-1757 | Important | Elevation of Privilege | No |
| MS15-063 | CVE-2015-1758 | Important | Elevation of Privilege | No |
| MS15-064 | CVE-2015-1764 | Important | Information Disclosure | No |
| MS15-064 | CVE-2015-1771 | Important | Elevation of Privilege | No |
| MS15-064 | CVE-2015-2359 | Important | Information Disclosure | No |
| MS15-065 | CVE-2015-1729 | Important | Information Disclosure | Yes |
| MS15-065 | CVE-2015-1733 | Critical | Remote Code Execution | Yes |
| MS15-065 | CVE-2015-1738 | Critical | Remote Code Execution | Yes |
| MS15-065 | CVE-2015-1767 | Critical | Remote Code Execution | Yes |
| MS15-065 | CVE-2015-2383 | Critical | Remote Code Execution | Yes |
| MS15-065 | CVE-2015-2384 | Critical | Remote Code Execution | Yes |
| MS15-065 | CVE-2015-2385 | Critical | Remote Code Execution | Yes |
| MS15-065 | CVE-2015-2388 | Critical | Remote Code Execution | Yes |
| MS15-065 | CVE-2015-2389 | Critical | Remote Code Execution | Yes |
| MS15-065 | CVE-2015-2390 | Critical | Remote Code Execution | Yes |
| MS15-065 | CVE-2015-2391 | Critical | Remote Code Execution | Yes |
| MS15-065 | CVE-2015-2397 | Critical | Remote Code Execution | Yes |
| MS15-065 | CVE-2015-2398 | Important | Security Feature Bypass | Yes |
| MS15-065 | CVE-2015-2401 | Critical | Remote Code Execution | Yes |
| MS15-065 | CVE-2015-2402 | Important | Elevation of Privilege | Yes |
| MS15-065 | CVE-2015-2403 | Critical | Remote Code Execution | Yes |
| MS15-065 | CVE-2015-2404 | Critical | Remote Code Execution | Yes |
| MS15-065 | CVE-2015-2406 | Critical | Remote Code Execution | Yes |
| MS15-065 | CVE-2015-2408 | Critical | Remote Code Execution | Yes |
| MS15-065 | CVE-2015-2410 | Important | Information Disclosure | Yes |
| MS15-065 | CVE-2015-2411 | Critical | Remote Code Execution | Yes |
| MS15-065 | CVE-2015-2412 | Important | Information Disclosure | Yes |
| MS15-065 | CVE-2015-2413 | Important | Information Disclosure | Yes |
| MS15-065 | CVE-2015-2414 | Important | Information Disclosure | Yes |
| MS15-065 | CVE-2015-2419 | Critical | Remote Code Execution | Yes |
| MS15-065 | CVE-2015-2421 | Important | Security Feature Bypass | Yes |
| MS15-065 | CVE-2015-2422 | Critical | Remote Code Execution | Yes |
| MS15-065 | CVE-2015-2425 | Critical | Remote Code Execution | Yes |
| MS15-066 | CVE-2015-2372 | Critical | Remote Code Execution | No |
| MS15-067 | CVE-2015-2373 | Critical | Remote Code Execution | No |
| MS15-068 | CVE-2015-2361 | Critical | Remote Code Execution | No |



| Bulletin | Vulnerability | Severity Rating | Impact | Mitigated |
|----------|---------------|-----------------|-------------------------|-----------|
| MS15-068 | CVE-2015-2362 | Critical | Remote Code Execution | No |
| MS15-069 | CVE-2015-2368 | Important | Remote Code Execution | No |
| MS15-069 | CVE-2015-2369 | Important | Remote Code Execution | No |
| MS15-070 | CVE-2015-2376 | Important | Remote Code Execution | Yes |
| MS15-070 | CVE-2015-2377 | Important | Remote Code Execution | Yes |
| MS15-070 | CVE-2015-2379 | Important | Remote Code Execution | Yes |
| MS15-070 | CVE-2015-2380 | Important | Remote Code Execution | Yes |
| MS15-070 | CVE-2015-2415 | Important | Remote Code Execution | Yes |
| MS15-070 | CVE-2015-2424 | Important | Remote Code Execution | Yes |
| MS15-070 | CVE-2015-2375 | Important | Remote Code Execution | Yes |
| MS15-070 | CVE-2015-2378 | Important | Remote Code Execution | Yes |
| MS15-071 | CVE-2015-2374 | Important | Elevation of Privilege | No |
| MS15-072 | CVE-2015-2364 | Important | Elevation of Privilege | No |
| MS15-073 | CVE-2015-2363 | Important | Elevation of Privilege | No |
| MS15-073 | CVE-2015-2365 | Important | Elevation of Privilege | No |
| MS15-073 | CVE-2015-2366 | Important | Elevation of Privilege | No |
| MS15-073 | CVE-2015-2367 | Important | Information Disclosure | No |
| MS15-073 | CVE-2015-2381 | Important | Information Disclosure | No |
| MS15-073 | CVE-2015-2382 | Important | Information Disclosure | No |
| MS15-074 | CVE-2015-2371 | Important | Elevation of Privilege | No |
| MS15-075 | CVE-2015-2416 | Important | Elevation of Privilege | No |
| MS15-075 | CVE-2015-2417 | Important | Elevation of Privilege | No |
| MS15-076 | CVE-2015-2370 | Important | Elevation of Privilege | No |
| MS15-077 | CVE-2015-2387 | Important | Elevation of Privilege | No |
| MS15-078 | CVE-2015-2426 | Critical | Remote Code Execution | No |
| MS15-079 | CVE-2015-2443 | Critical | Remote Code Execution | Yes |
| MS15-079 | CVE-2015-2444 | Critical | Remote Code Execution | Yes |
| MS15-079 | CVE-2015-2445 | Critical | Security Feature Bypass | Yes |
| MS15-079 | CVE-2015-2447 | Critical | Remote Code Execution | Yes |
| MS15-079 | CVE-2015-2448 | Critical | Remote Code Execution | Yes |
| MS15-079 | CVE-2015-2451 | Critical | Remote Code Execution | Yes |
| MS15-079 | CVE-2015-2452 | Critical | Remote Code Execution | Yes |
| MS15-080 | CVE-2015-2432 | Critical | Remote Code Execution | No |
| MS15-080 | CVE-2015-2458 | Critical | Remote Code Execution | No |
| MS15-080 | CVE-2015-2459 | Critical | Remote Code Execution | No |
| MS15-080 | CVE-2015-2460 | Critical | Remote Code Execution | No |
| MS15-080 | CVE-2015-2461 | Critical | Remote Code Execution | No |
| MS15-080 | CVE-2015-2462 | Critical | Remote Code Execution | No |
| MS15-080 | CVE-2015-2455 | Critical | Remote Code Execution | No |



| Bulletin | Vulnerability | Severity Rating | Impact | Mitigated |
|----------|---------------|-----------------|-------------------------|-----------|
| MS15-080 | CVE-2015-2456 | Critical | Remote Code Execution | No |
| MS15-080 | CVE-2015-2463 | Critical | Remote Code Execution | No |
| MS15-080 | CVE-2015-2464 | Critical | Remote Code Execution | No |
| MS15-080 | CVE-2015-2433 | Important | Security Feature Bypass | No |
| MS15-080 | CVE-2015-2453 | Important | Elevation of Privilege | No |
| MS15-080 | CVE-2015-2454 | Important | Elevation of Privilege | No |
| MS15-080 | CVE-2015-2465 | Important | Security Feature Bypass | No |
| MS15-080 | CVE-2015-2431 | Critical | Remote Code Execution | No |
| MS15-080 | CVE-2015-2435 | Critical | Remote Code Execution | No |
| MS15-081 | CVE-2015-1642 | Important | Remote Code Execution | Yes |
| MS15-081 | CVE-2015-2466 | Critical | Remote Code Execution | Yes |
| MS15-081 | CVE-2015-2467 | Important | Remote Code Execution | Yes |
| MS15-081 | CVE-2015-2468 | Important | Remote Code Execution | Yes |
| MS15-081 | CVE-2015-2469 | Important | Remote Code Execution | Yes |
| MS15-081 | CVE-2015-2470 | Important | Remote Code Execution | Yes |
| MS15-081 | CVE-2015-2477 | Important | Remote Code Execution | Yes |
| MS15-082 | CVE-2015-2472 | Important | Spoofing | No |
| MS15-082 | CVE-2015-2473 | Important | Remote Code Execution | No |
| MS15-083 | CVE-2015-2474 | Important | Remote Code Execution | No |
| MS15-084 | CVE-2015-2434 | Important | Information Disclosure | No |
| MS15-084 | CVE-2015-2440 | Important | Information Disclosure | No |
| MS15-084 | CVE-2015-2471 | Important | Information Disclosure | No |
| MS15-085 | CVE-2015-1769 | Important | Elevation of Privilege | No |
| MS15-086 | CVE-2015-2420 | Important | Elevation of Privilege | No |
| MS15-087 | CVE-2015-2475 | Important | Elevation of Privilege | No |
| MS15-088 | CVE-2015-2423 | Important | Information Disclosure | Yes |
| MS15-089 | CVE-2015-2476 | Important | Information Disclosure | No |
| MS15-090 | CVE-2015-2428 | Important | Elevation of Privilege | No |
| MS15-090 | CVE-2015-2429 | Important | Elevation of Privilege | No |
| MS15-090 | CVE-2015-2430 | Important | Elevation of Privilege | No |
| MS15-091 | CVE-2015-2441 | Critical | Remote Code Execution | Yes |
| MS15-091 | CVE-2015-2442 | Critical | Remote Code Execution | Yes |
| MS15-091 | CVE-2015-2446 | Critical | Remote Code Execution | Yes |
| MS15-091 | CVE-2015-2449 | Important | Security Feature Bypass | Yes |
| MS15-092 | CVE-2015-2479 | Important | Elevation of Privilege | Yes |
| MS15-092 | CVE-2015-2480 | Important | Elevation of Privilege | Yes |
| MS15-092 | CVE-2015-2481 | Important | Elevation of Privilege | Yes |
| MS15-093 | CVE-2015-2502 | Critical | Remote Code Execution | Yes |
| MS15-094 | CVE-2015-2483 | Important | Information Disclosure | Yes |



| Bulletin | Vulnerability | Severity Rating | Impact | Mitigated |
|----------|---------------|-----------------|-------------------------|-----------|
| MS15-094 | CVE-2015-2484 | Important | Information Disclosure | Yes |
| MS15-094 | CVE-2015-2487 | Critical | Remote Code Execution | Yes |
| MS15-094 | CVE-2015-2489 | Important | Elevation of Privilege | Yes |
| MS15-094 | CVE-2015-2490 | Critical | Remote Code Execution | Yes |
| MS15-094 | CVE-2015-2491 | Critical | Remote Code Execution | Yes |
| MS15-094 | CVE-2015-2492 | Critical | Remote Code Execution | Yes |
| MS15-094 | CVE-2015-2493 | Critical | Remote Code Execution | Yes |
| MS15-094 | CVE-2015-2498 | Critical | Remote Code Execution | Yes |
| MS15-094 | CVE-2015-2499 | Critical | Remote Code Execution | Yes |
| MS15-094 | CVE-2015-2500 | Critical | Remote Code Execution | Yes |
| MS15-094 | CVE-2015-2501 | Critical | Remote Code Execution | Yes |
| MS15-094 | CVE-2015-2541 | Critical | Remote Code Execution | Yes |
| MS15-095 | CVE-2015-2485 | Critical | Remote Code Execution | Yes |
| MS15-095 | CVE-2015-2486 | Critical | Remote Code Execution | Yes |
| MS15-095 | CVE-2015-2494 | Critical | Remote Code Execution | Yes |
| MS15-095 | CVE-2015-2542 | Critical | Remote Code Execution | Yes |
| MS15-096 | CVE-2015-2535 | Important | Denial of Service | No |
| MS15-097 | CVE-2015-2506 | Important | Elevation of Privilege | No |
| MS15-097 | CVE-2015-2507 | Important | Elevation of Privilege | No |
| MS15-097 | CVE-2015-2508 | Important | Elevation of Privilege | No |
| MS15-097 | CVE-2015-2510 | Critical | Remote Code Execution | No |
| MS15-097 | CVE-2015-2511 | Important | Elevation of Privilege | No |
| MS15-097 | CVE-2015-2512 | Important | Elevation of Privilege | No |
| MS15-097 | CVE-2015-2517 | Important | Elevation of Privilege | No |
| MS15-097 | CVE-2015-2518 | Important | Elevation of Privilege | No |
| MS15-097 | CVE-2015-2527 | Important | Elevation of Privilege | No |
| MS15-097 | CVE-2015-2529 | Important | Security Feature Bypass | No |
| MS15-097 | CVE-2015-2546 | Important | Elevation of Privilege | No |
| MS15-098 | CVE-2015-2513 | Critical | Remote Code Execution | Yes |
| MS15-098 | CVE-2015-2514 | Low | Denial of Service | Yes |
| MS15-098 | CVE-2015-2516 | Low | Denial of Service | Yes |
| MS15-098 | CVE-2015-2519 | Critical | Remote Code Execution | Yes |
| MS15-098 | CVE-2015-2530 | Critical | Remote Code Execution | Yes |
| MS15-099 | CVE-2015-2520 | Important | Remote Code Execution | Yes |
| MS15-099 | CVE-2015-2521 | Important | Remote Code Execution | Yes |
| MS15-099 | CVE-2015-2523 | Important | Remote Code Execution | Yes |
| MS15-099 | CVE-2015-2545 | Critical | Remote Code Execution | Yes |
| MS15-100 | CVE-2015-2509 | Important | Remote Code Execution | Yes |
| MS15-101 | CVE-2015-2504 | Important | Elevation of Privilege | Yes |



| Bulletin | Vulnerability | Severity Rating | Impact | Mitigated |
|----------|---------------|-----------------|-------------------------|-----------|
| MS15-101 | CVE-2015-2526 | Important | Denial of Service | No |
| MS15-102 | CVE-2015-2524 | Important | Elevation of Privilege | No |
| MS15-102 | CVE-2015-2525 | Important | Elevation of Privilege | No |
| MS15-102 | CVE-2015-2528 | Important | Elevation of Privilege | No |
| MS15-103 | CVE-2015-2505 | Important | Information Disclosure | No |
| MS15-103 | CVE-2015-2543 | Important | Spoofing | No |
| MS15-103 | CVE-2015-2544 | Important | Spoofing | No |
| MS15-104 | CVE-2015-2531 | Important | Information Disclosure | No |
| MS15-104 | CVE-2015-2532 | Important | Information Disclosure | No |
| MS15-104 | CVE-2015-2536 | Important | Elevation of Privilege | No |
| MS15-105 | CVE-2015-2534 | Important | Security Feature Bypass | No |
| MS15-106 | CVE-2015-6042 | Critical | Remote Code Execution | Yes |
| MS15-106 | CVE-2015-6044 | Important | Elevation of Privilege | Yes |
| MS15-106 | CVE-2015-6045 | Critical | Remote Code Execution | Yes |
| MS15-106 | CVE-2015-6046 | Critical | Remote Code Execution | Yes |
| MS15-106 | CVE-2015-6047 | Important | Elevation of Privilege | Yes |
| MS15-106 | CVE-2015-6048 | Critical | Remote Code Execution | Yes |
| MS15-106 | CVE-2015-6049 | Critical | Remote Code Execution | Yes |
| MS15-106 | CVE-2015-6050 | Critical | Remote Code Execution | Yes |
| MS15-106 | CVE-2015-6051 | Important | Elevation of Privilege | Yes |
| MS15-106 | CVE-2015-6053 | Important | Information Disclosure | Yes |
| MS15-106 | CVE-2015-6056 | Critical | Remote Code Execution | Yes |
| MS15-107 | CVE-2015-6057 | Important | Information Disclosure | Yes |
| MS15-107 | CVE-2015-6058 | Important | Security Feature Bypass | Yes |
| MS15-108 | CVE-2015-2482 | Critical | Remote Code Execution | Yes |
| MS15-108 | CVE-2015-6052 | Important | Security Feature Bypass | Yes |
| MS15-108 | CVE-2015-6055 | Critical | Remote Code Execution | Yes |
| MS15-108 | CVE-2015-6059 | Important | Information Disclosure | Yes |
| MS15-109 | CVE-2015-2515 | Critical | Remote Code Execution | Yes |
| MS15-109 | CVE-2015-2548 | Critical | Remote Code Execution | No |
| MS15-110 | CVE-2015-2555 | Important | Remote Code Execution | Yes |
| MS15-110 | CVE-2015-2557 | Important | Remote Code Execution | Yes |
| MS15-110 | CVE-2015-2558 | Important | Remote Code Execution | Yes |
| MS15-110 | CVE-2015-6037 | Important | Spoofing | Yes |
| MS15-110 | CVE-2015-2556 | Important | Information Disclosure | Yes |
| MS15-110 | CVE-2015-6039 | Important | Security Feature Bypass | Yes |
| MS15-111 | CVE-2015-2549 | Important | Elevation of Privilege | No |
| MS15-111 | CVE-2015-2550 | Important | Elevation of Privilege | No |
| MS15-111 | CVE-2015-2552 | Important | Security Feature Bypass | No |



| Bulletin | Vulnerability | Severity Rating | Impact | Mitigated |
|----------|---------------|-----------------|-------------------------|-----------|
| MS15-111 | CVE-2015-2553 | Important | Elevation of Privilege | No |
| MS15-111 | CVE-2015-2554 | Important | Elevation of Privilege | No |
| MS15-112 | CVE-2015-2427 | Critical | Remote Code Execution | Yes |
| MS15-112 | CVE-2015-6065 | Critical | Remote Code Execution | Yes |
| MS15-112 | CVE-2015-6066 | Critical | Remote Code Execution | Yes |
| MS15-112 | CVE-2015-6068 | Critical | Remote Code Execution | Yes |
| MS15-112 | CVE-2015-6069 | Critical | Remote Code Execution | Yes |
| MS15-112 | CVE-2015-6070 | Critical | Remote Code Execution | Yes |
| MS15-112 | CVE-2015-6071 | Critical | Remote Code Execution | Yes |
| MS15-112 | CVE-2015-6072 | Critical | Remote Code Execution | Yes |
| MS15-112 | CVE-2015-6074 | Critical | Remote Code Execution | Yes |
| MS15-112 | CVE-2015-6075 | Critical | Remote Code Execution | Yes |
| MS15-112 | CVE-2015-6076 | Critical | Remote Code Execution | Yes |
| MS15-112 | CVE-2015-6077 | Critical | Remote Code Execution | Yes |
| MS15-112 | CVE-2015-6079 | Critical | Remote Code Execution | Yes |
| MS15-112 | CVE-2015-6080 | Critical | Remote Code Execution | Yes |
| MS15-112 | CVE-2015-6081 | Critical | Remote Code Execution | Yes |
| MS15-112 | CVE-2015-6082 | Critical | Remote Code Execution | Yes |
| MS15-112 | CVE-2015-6084 | Critical | Remote Code Execution | Yes |
| MS15-112 | CVE-2015-6085 | Critical | Remote Code Execution | Yes |
| MS15-112 | CVE-2015-6086 | Important | Information Disclosure | Yes |
| MS15-112 | CVE-2015-6087 | Critical | Remote Code Execution | Yes |
| MS15-112 | CVE-2015-6089 | Critical | Remote Code Execution | Yes |
| MS15-113 | CVE-2015-6064 | Critical | Remote Code Execution | Yes |
| MS15-113 | CVE-2015-6073 | Critical | Remote Code Execution | Yes |
| MS15-113 | CVE-2015-6078 | Critical | Remote Code Execution | Yes |
| MS15-113 | CVE-2015-6088 | Important | Security Feature Bypass | Yes |
| MS15-114 | CVE-2015-6097 | Critical | Remote Code Execution | Yes |
| MS15-115 | CVE-2015-6100 | Important | Elevation of Privilege | No |
| MS15-115 | CVE-2015-6101 | Important | Elevation of Privilege | No |
| MS15-115 | CVE-2015-6102 | Important | Information Disclosure | No |
| MS15-115 | CVE-2015-6103 | Critical | Remote Code Execution | No |
| MS15-115 | CVE-2015-6104 | Critical | Remote Code Execution | No |
| MS15-115 | CVE-2015-6109 | Important | Information Disclosure | No |
| MS15-115 | CVE-2015-6113 | Important | Security Feature Bypass | No |
| MS15-116 | CVE-2015-2503 | Important | Elevation of Privilege | Yes |
| MS15-116 | CVE-2015-6038 | Important | Remote Code Execution | Yes |
| MS15-116 | CVE-2015-6091 | Important | Remote Code Execution | Yes |
| MS15-116 | CVE-2015-6092 | Important | Remote Code Execution | Yes |



| Bulletin | Vulnerability | Severity Rating | Impact | Mitigated |
|----------|---------------|-----------------|-------------------------|-----------|
| MS15-116 | CVE-2015-6093 | Important | Remote Code Execution | Yes |
| MS15-116 | CVE-2015-6094 | Important | Remote Code Execution | Yes |
| MS15-116 | CVE-2015-6123 | Important | Spoofing | Yes |
| MS15-117 | CVE-2015-6098 | Important | Elevation of Privilege | No |
| MS15-118 | CVE-2015-6096 | Important | Information Disclosure | No |
| MS15-118 | CVE-2015-6099 | Important | Elevation of Privilege | No |
| MS15-118 | CVE-2015-6115 | Important | Security Feature Bypass | No |
| MS15-119 | CVE-2015-2478 | Important | Elevation of Privilege | No |
| MS15-120 | CVE-2015-6111 | Important | Denial of Service | No |
| MS15-121 | CVE-2015-6112 | Important | Spoofing | No |
| MS15-122 | CVE-2015-6095 | Important | Security Feature Bypass | No |
| MS15-123 | CVE-2015-6061 | Important | Information Disclosure | No |
| MS15-124 | CVE-2015-6083 | Critical | Remote Code Execution | Yes |
| MS15-124 | CVE-2015-6134 | Critical | Remote Code Execution | Yes |
| MS15-124 | CVE-2015-6138 | Moderate | Security Feature Bypass | Yes |
| MS15-124 | CVE-2015-6141 | Critical | Remote Code Execution | Yes |
| MS15-124 | CVE-2015-6143 | Critical | Remote Code Execution | Yes |
| MS15-124 | CVE-2015-6144 | Moderate | Security Feature Bypass | Yes |
| MS15-124 | CVE-2015-6145 | Critical | Remote Code Execution | Yes |
| MS15-124 | CVE-2015-6146 | Critical | Remote Code Execution | Yes |
| MS15-124 | CVE-2015-6147 | Critical | Remote Code Execution | Yes |
| MS15-124 | CVE-2015-6149 | Critical | Remote Code Execution | Yes |
| MS15-124 | CVE-2015-6150 | Critical | Remote Code Execution | Yes |
| MS15-124 | CVE-2015-6152 | Critical | Remote Code Execution | Yes |
| MS15-124 | CVE-2015-6156 | Critical | Remote Code Execution | Yes |
| MS15-124 | CVE-2015-6157 | Important | Information Disclosure | Yes |
| MS15-124 | CVE-2015-6160 | Critical | Remote Code Execution | Yes |
| MS15-124 | CVE-2015-6162 | Critical | Remote Code Execution | Yes |
| MS15-124 | CVE-2015-6164 | Important | Security Feature Bypass | Yes |
| MS15-125 | CVE-2015-6139 | Important | Elevation of Privilege | Yes |
| MS15-125 | CVE-2015-6140 | Critical | Remote Code Execution | Yes |
| MS15-125 | CVE-2015-6142 | Critical | Remote Code Execution | Yes |
| MS15-125 | CVE-2015-6148 | Critical | Remote Code Execution | Yes |
| MS15-125 | CVE-2015-6151 | Critical | Remote Code Execution | Yes |
| MS15-125 | CVE-2015-6153 | Critical | Remote Code Execution | Yes |
| MS15-125 | CVE-2015-6154 | Critical | Remote Code Execution | Yes |
| MS15-125 | CVE-2015-6155 | Critical | Remote Code Execution | Yes |
| MS15-125 | CVE-2015-6158 | Critical | Remote Code Execution | Yes |
| MS15-125 | CVE-2015-6159 | Critical | Remote Code Execution | Yes |



| Bulletin | Vulnerability | Severity Rating | Impact | Mitigated |
|----------|---------------|-----------------|-------------------------|-----------|
| MS15-125 | CVE-2015-6161 | Important | Security Feature Bypass | Yes |
| MS15-125 | CVE-2015-6168 | Critical | Remote Code Execution | Yes |
| MS15-125 | CVE-2015-6169 | Important | Spoofing | Yes |
| MS15-125 | CVE-2015-6170 | Important | Elevation of Privilege | Yes |
| MS15-125 | CVE-2015-6176 | Moderate | Information Disclosure | Yes |
| MS15-126 | CVE-2015-6135 | Important | Information Disclosure | Yes |
| MS15-126 | CVE-2015-6136 | Critical | Remote Code Execution | Yes |
| MS15-127 | CVE-2015-6125 | Critical | Remote Code Execution | No |
| MS15-128 | CVE-2015-6106 | Critical | Remote Code Execution | No |
| MS15-128 | CVE-2015-6107 | Critical | Remote Code Execution | No |
| MS15-128 | CVE-2015-6108 | Critical | Remote Code Execution | No |
| MS15-129 | CVE-2015-6114 | Important | Information Disclosure | No |
| MS15-129 | CVE-2015-6165 | Important | Information Disclosure | No |
| MS15-129 | CVE-2015-6166 | Critical | Remote Code Execution | Yes |
| MS15-130 | CVE-2015-6130 | Critical | Remote Code Execution | No |
| MS15-131 | CVE-2015-6040 | Important | Remote Code Execution | Yes |
| MS15-131 | CVE-2015-6118 | Important | Remote Code Execution | Yes |
| MS15-131 | CVE-2015-6122 | Important | Remote Code Execution | Yes |
| MS15-131 | CVE-2015-6124 | Important | Remote Code Execution | Yes |
| MS15-131 | CVE-2015-6172 | Critical | Remote Code Execution | Yes |
| MS15-131 | CVE-2015-6177 | Important | Remote Code Execution | Yes |
| MS15-132 | CVE-2015-6128 | Important | Remote Code Execution | Yes |
| MS15-132 | CVE-2015-6132 | Important | Remote Code Execution | Yes |
| MS15-132 | CVE-2015-6133 | Important | Remote Code Execution | Yes |
| MS15-133 | CVE-2015-6126 | Important | Elevation of Privilege | No |
| MS15-134 | CVE-2015-6127 | Important | Remote Code Execution | Yes |
| MS15-134 | CVE-2015-6131 | Important | Remote Code Execution | Yes |
| MS15-135 | CVE-2015-6171 | Important | Elevation of Privilege | No |
| MS15-135 | CVE-2015-6173 | Important | Elevation of Privilege | No |
| MS15-135 | CVE-2015-6174 | Important | Elevation of Privilege | No |
| MS15-135 | CVE-2015-6175 | Important | Elevation of Privilege | No |