Avecto Report

2016 Microsoft Vulnerabilities Study:

Mitigating risk by removing user privileges

Avecto Report

Contents

Executive summary

Analysis of Microsoft "Patch Tuesday" Security Bulletins from 2016 reveals that 94% of Critical Microsoft vulnerabilities would be mitigated by removing admin rights across an organization, up on last year's figure of 85%.

There were 530 vulnerabilities recorded in total, up slightly on the 524 last year but representing an increase of over 60% since 2013.

Despite being Microsoft's newest and 'most secure' operating system to date, Windows 10 was found to have the highest proportion of vulnerabilities of any OS (395), 46% more than Windows 8 and Windows 8.1 (265 each).

Introduction

Compiled by Avecto, this report analyses the data from security bulletins issued by Microsoft throughout 2016. 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.

With the release of Windows 10, Microsoft reduced the response time between vulnerability discovery (Zero Day) and the patch being rolled out, by releasing them as soon as they are available.

The 2016 Microsoft Vulnerabilities Report is the fourth version of Avecto's research. During this period the number of vulnerabilities has risen by 60%, from 333 to 530.

In 2015, there were a total of 251 Critical vulnerabilities, this dropped to 189 in 2016, while in 2014 there were 240.

The report finds that the risk associated with 94% 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 "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" or "If the current user is logged on with administrative user rights, an attacker could take control of an affected system" 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 2016 report highlights the following key findings:

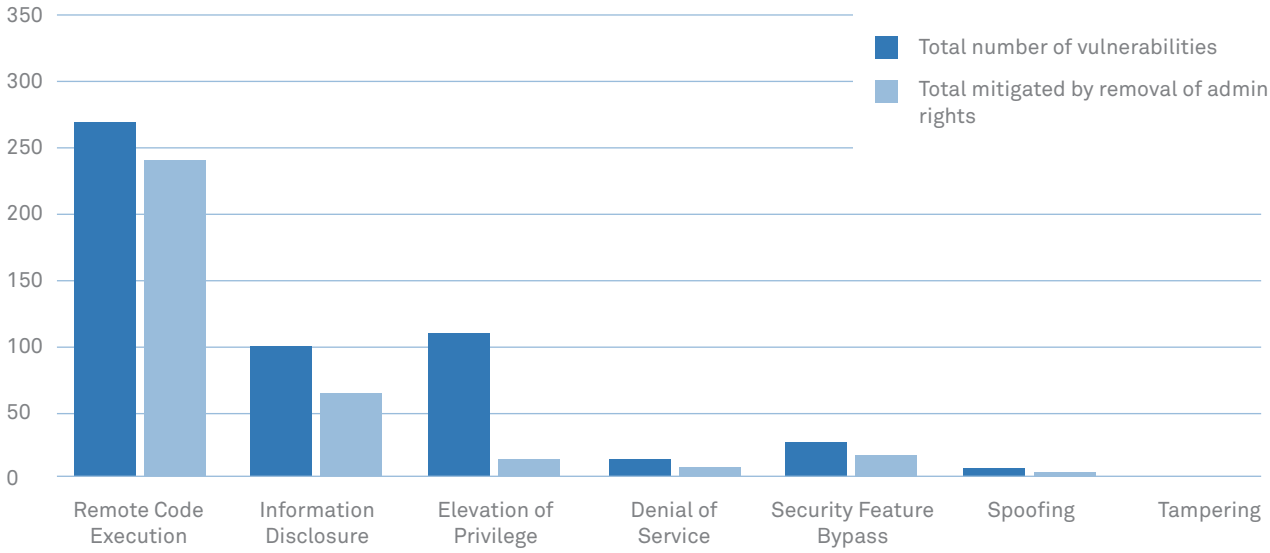
- Of the 189 vulnerabilities in 2016 with a Critical rating, 94% were concluded to be mitigated by removing administrator rights
- 66% of all Microsoft vulnerabilities reported in 2016 could be mitigated by removing admin rights
- There has been a 62% rise in the total volume of vulnerabilities since 2013
- 100% of vulnerabilities impacting Microsoft's latest browser Edge could be mitigated
- 100% of vulnerabilities in Internet Explorer could be mitigated by removing admin rights
- 99% of vulnerabilities affecting Microsoft Office could be mitigated by removing admin rights
- Despite being labelled as the "most secure" Windows OS ever, Windows 10 had the highest proportion of vulnerabilities (395) compared to any other OS.
- The volume of Windows 10 vulnerabilities was 46% higher than Windows 8 and Windows 8.1
- 93% Critical vulnerabilities affecting Windows 10 could be mitigated by removing admin rights
- From 2013 to 2016, there was a 63% increase in the total number of Windows vulnerabilities reported

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 2016 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 (RCE) vulnerabilities account for the largest proportion of total Microsoft vulnerabilities. Of these, 70% were classed as Critical. Almost 90% of total RCE vulnerabilities and 94% of Critical RCE vulnerabilities could be mitigated by removal of admin rights.

Breakdown of Microsoft Vulnerability Categories in 2016

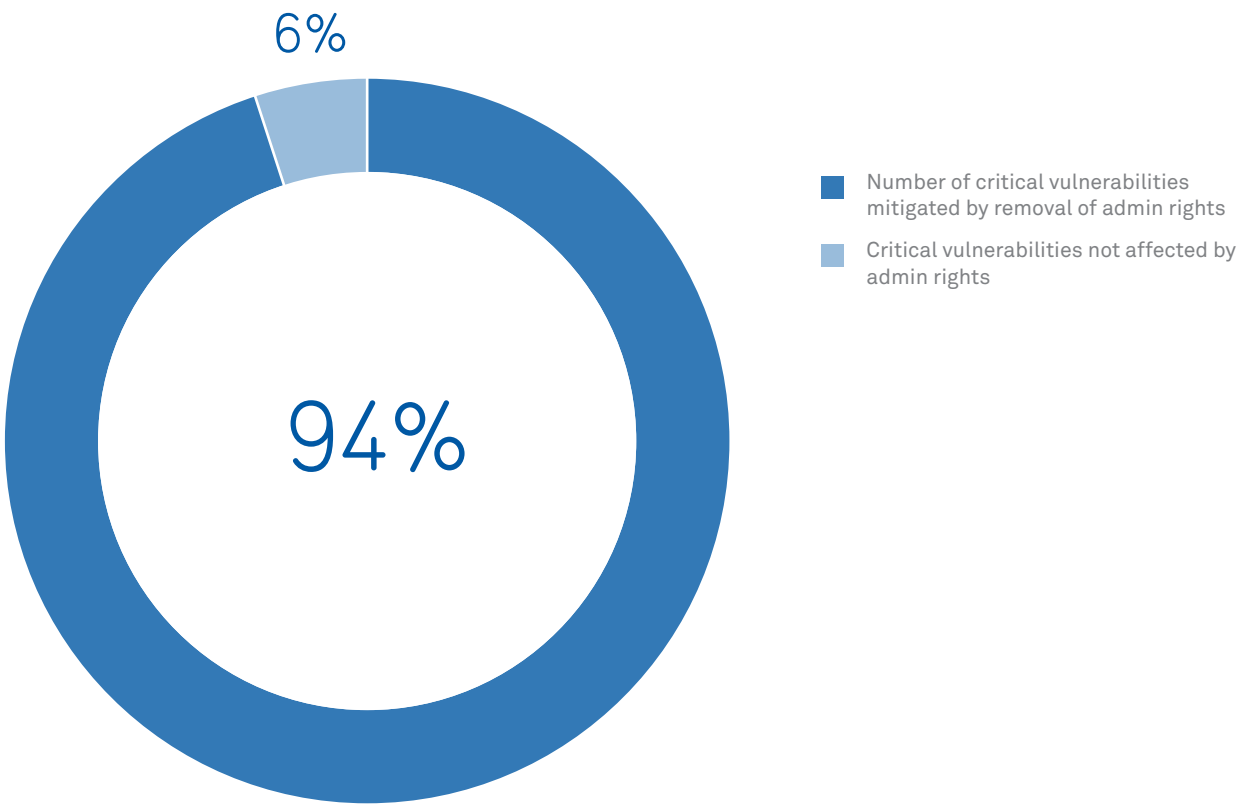


Microsoft Windows vulnerabilities

In 2016, 416 vulnerabilities were reported across Windows Vista, Windows 7, Windows RT, Windows 8 / 8.1 and Windows 10 operating systems compared to 433 in 2015 and 300 in 2014.

94% of Critical vulnerabilities affecting Microsoft Windows in 2016 could be mitigated by the removal of admin rights

Critical Windows vulnerabilities mitigated by removal of admin rights in 2016



Microsoft Edge

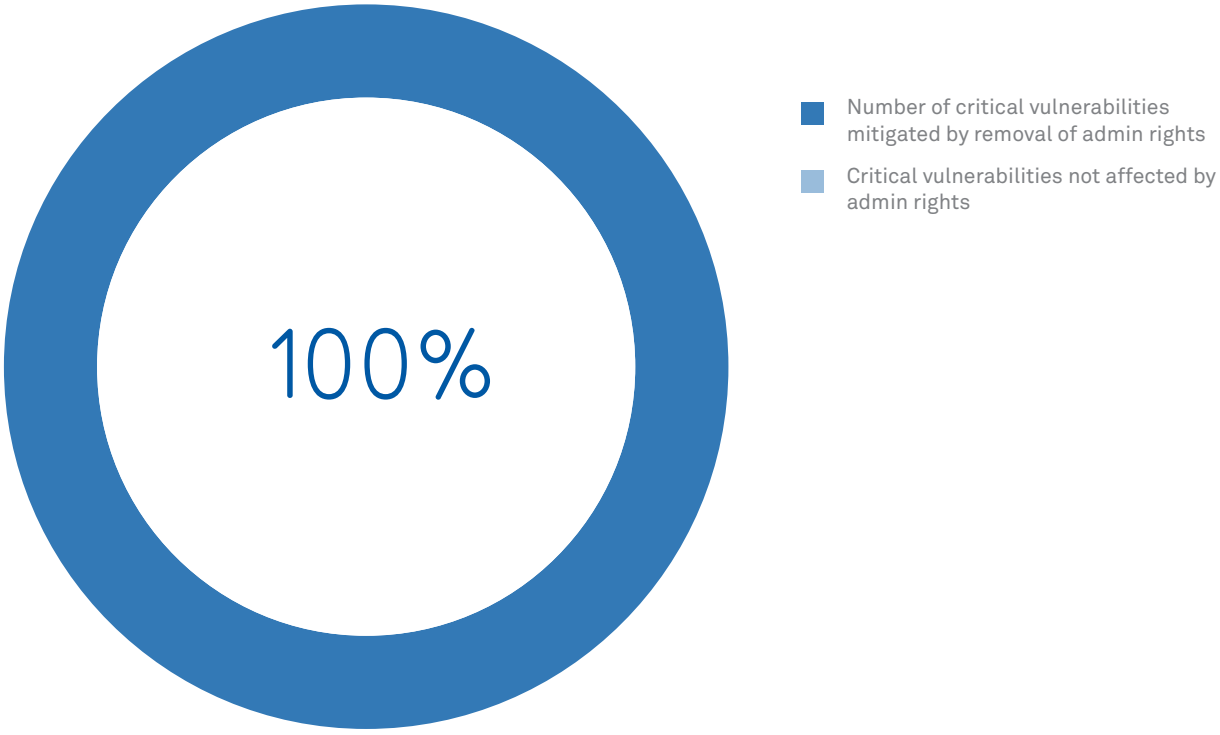
Removing admin rights is critical to keeping Microsoft's new Edge browser secure. A total of 111 vulnerabilities, 68 Critical, affected the browser and 100% could be mitigated.

Internet Explorer

In 2016, 109 vulnerabilities were reported that affected Internet Explorer (IE) versions 6 -11, compared to 238 the previous year.

100% of IE vulnerabilities in 2016 could be mitigated by the removal of user admin rights.

Internet Explorer vulnerabilities mitigated by removal of admin rights in 2016



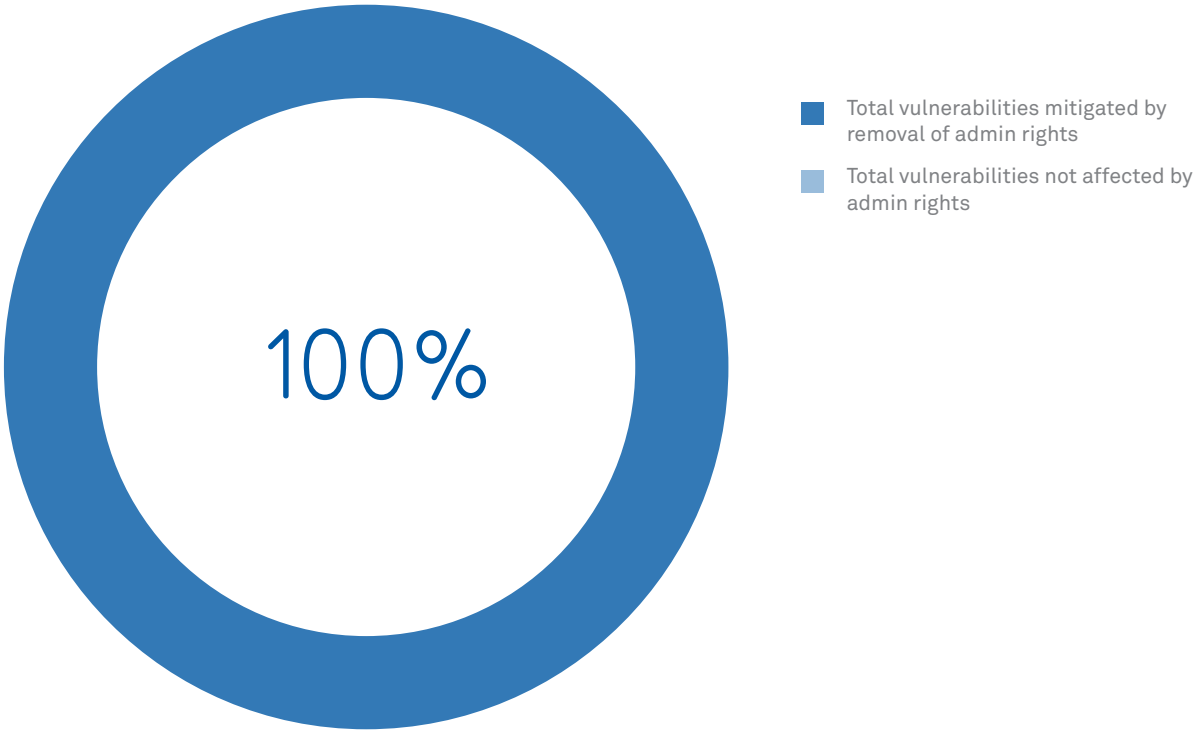
Microsoft Office

Microsoft Security Bulletins in 2016 published 79 vulnerabilities affecting Microsoft Office products, compared to 62 in 2015 and just 20 in 2014.

This data includes Office 2010, Office 2013, Office 2016, Microsoft Excel, Word, PowerPoint, Visio and Publisher amongst others. Removing admin rights would mitigate 99% of these Office vulnerabilities.

100% of those vulnerabilities in Office 2016, the latest version of Microsoft's software, were mitigated by removing admin rights.

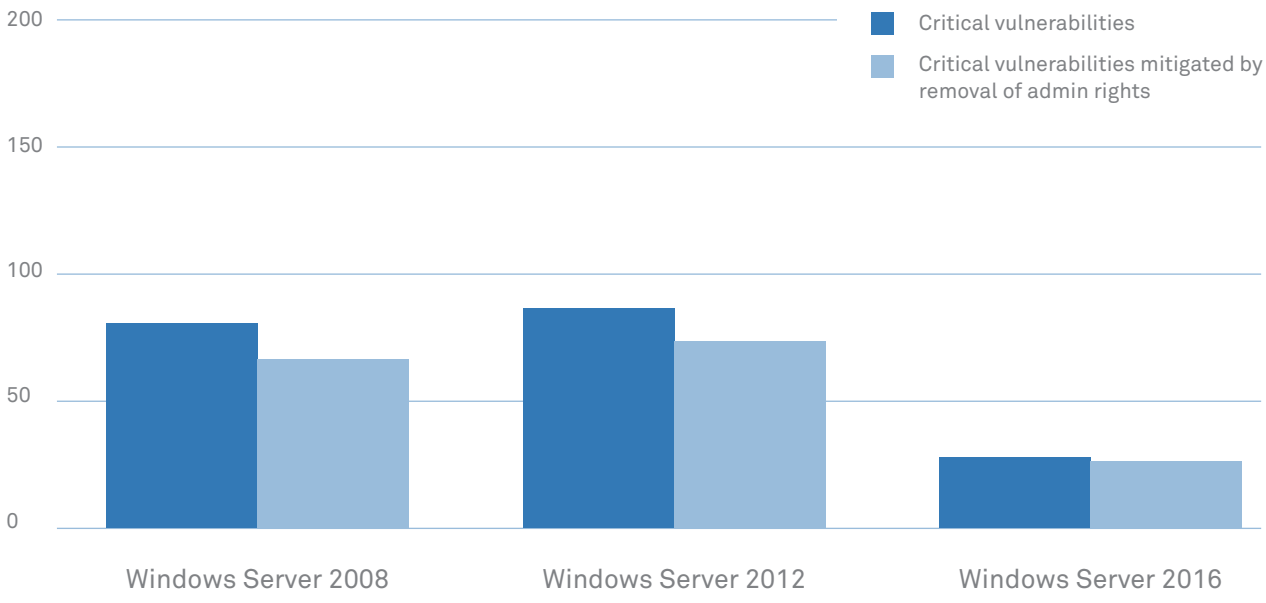
Office 2016 vulnerabilities mitigated by removal of admin rights



Windows Server vulnerabilities

319 vulnerabilities were reported in Microsoft Security Bulletins affecting Microsoft Windows Server in 2016. Of the 108 vulnerabilities with a Critical rating, 90% were mitigated by the removal of admin rights.

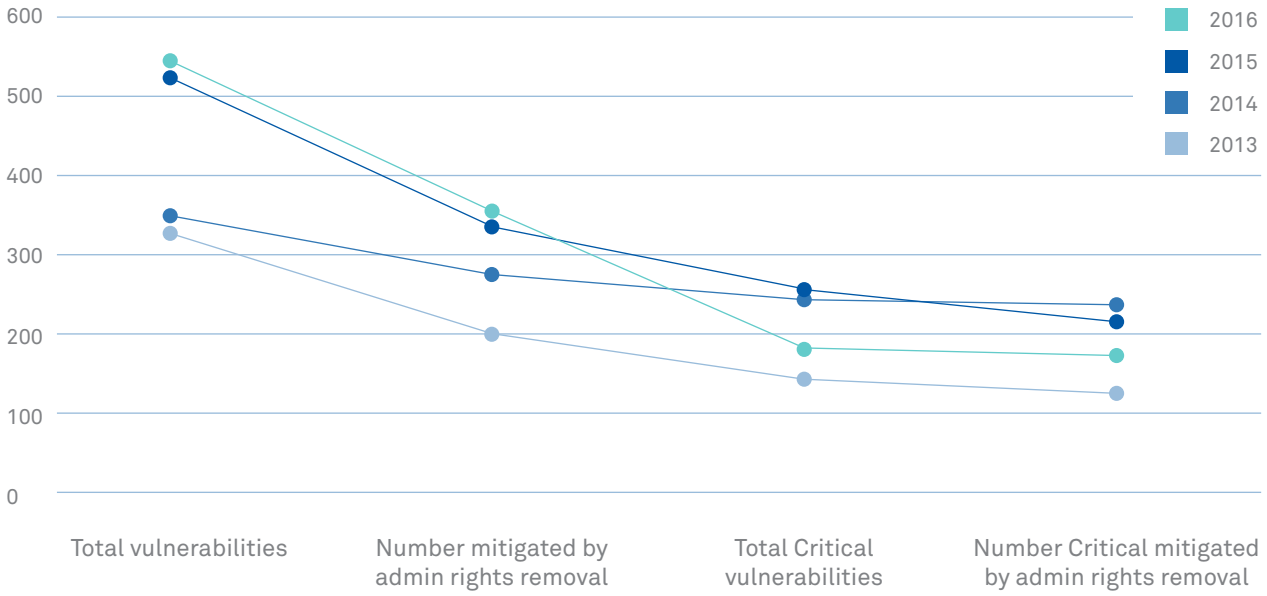
Critical Windows Server vulnerabilities mitigated by removal of admin rights



Conclusion

The figures from the 2016 Microsoft Vulnerabilities Study once again highlight the importance of removing admin rights.

Trends 2013-2016



The percentage of vulnerabilities mitigated by removing admin rights increased in 2016, but has remained at a fairly steady level across the last four years.

However, since 2013 the overall number of vulnerabilities has increased significantly, giving organizations ecreating a growing challenge for organizations to manage their patching strategies.

Attacks are growing ever-more sophisticated, targeted and hard to detect. In 93% of cases, it took attackers minutes or less to compromise systems (Verizon DBIR 2016).

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.

Defendpoint's proactive prevention offers multi-layered protection to stop cyber attacks. Implementing a proactive defense strategy, starting at the endpoint and building out with least privilege, simple application whitelisting and content isolation will put you in a much stronger position by reducing the attack surface and building secure defensible endpoints.

This method works alongside tools such as antivirus to proactively prevent malware from executing in the first place, rather than relying on detection and response after the event. This allows you to implement a robust defense in depth strategy.

"Admin access to a local endpoint is the first step to accessing the whole company and its confidential data. To prevent insider threats companies need to start by limiting the administrative rights on endpoints."

Sami Laiho
Windows security expert
and Microsoft MVP

About Defendpoint

Defendpoint by Avecto is a multi-layered prevention engine that stops cyber attacks at the endpoint. Its unique and proactive approach integrates three core capabilities of privilege management, application control and content isolation. This innovative solution allows organizations to balance security and usability, ensuring user experience is never compromised.

It allows you to create a solid security foundation by focusing on the application layer of the endpoint security stack. Automatically isolate applications working with untrusted content to protect data and Critical resources. Pragmatic application control rules ensure only known and trusted applications are allowed to run on the endpoint, and block the unknown with comprehensive exception-handling. Remove admin rights and assign privileges to tasks to mitigate attacks that hit the operating system.

Defendpoint takes a proactive approach to defending the endpoint when antimalware fails.

Appendix 1: Detailed Methodology

Data source

This report has been compiled following analysis of the Security bulletins published in 2016 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”, or similar variations, are 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.

Certain vulnerabilities have appeared in multiple bulletins throughout 2016, 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: **https://technet.microsoft.com/en-us/library/security/mt637763.aspx**

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.

Bulletin	Mitigated	Vulnerability	Severity Rating	Impact
MS16-001	Yes	CVE-2016-0002	Critical	Remote Code Execution
MS16-001	Yes	CVE-2016-0005	Important	Elevation of Privilege
MS16-002	Yes	CVE-2016-0003	Critical	Remote Code Execution
MS16-002	Yes	CVE-2016-0024	Critical	Remote Code Execution
MS16-003	Yes	CVE-2016-0002	Critical	Remote Code Execution
MS16-004	Yes	CVE-2016-0010	Critical	Remote Code Execution
MS16-004	Yes	CVE-2016-0012	Important	Security Feature Bypass
MS16-004	Yes	CVE-2016-0035	Important	Remote Code Execution
MS16-004	Yes	CVE-2016-0011	Important	Security Feature Bypass
MS16-004	Yes	CVE-2015-6117	Important	Security Feature Bypass
MS16-004	Yes	CVE-2016-0012	Important	Security Feature Bypass
MS16-005	Yes	CVE-2016-0009	Critical	Remote Code Execution
MS16-005	No	CVE-2016-0008	Important	Information Disclosure
MS16-006	Yes	CVE-2016-0034	Critical	Remote Code Execution
MS16-007	No	CVE-2016-0014	Important	Elevation of Privilege
MS16-007	Yes	CVE-2016-0015	Important	Remote Code Execution
MS16-007	No	CVE-2016-0016	Important	Remote Code Execution
MS16-007	No	CVE-2016-0018	Important	Remote Code Execution
MS16-007	No	CVE-2016-0019	Important	Security Feature Bypass
MS16-007	No	CVE-2016-0020	Important	Elevation of Privilege
MS16-008	No	CVE-2016-0006	Important	Elevation of Privilege
MS16-008	No	CVE-2016-0007	Important	Elevation of Privilege
MS16-009	Yes	CVE-2016-0041	Important	Remote Code Execution
MS16-009	Yes	CVE-2016-0059	Important	Information Disclosure
MS16-009	Yes	CVE-2016-0060	Critical	Remote Code Execution
MS16-009	Yes	CVE-2016-0061	Critical	Remote Code Execution
MS16-009	Yes	CVE-2016-0062	Critical	Remote Code Execution
MS16-009	Yes	CVE-2016-0063	Critical	Remote Code Execution
MS16-009	Yes	CVE-2016-0064	Critical	Remote Code Execution

Bulletin	Mitigated	Vulnerability	Severity Rating	Impact
MS16-009	Yes	CVE-2016-0067	Critical	Remote Code Execution
MS16-009	Yes	CVE-2016-0068	Important	Elevation of Privilege
MS16-009	Yes	CVE-2016-0069	Important	Elevation of Privilege
MS16-009	Yes	CVE-2016-0071	Important	Remote Code Execution
MS16-009	Yes	CVE-2016-0072	Critical	Remote Code Execution
MS16-009	Yes	CVE-2016-0077	Moderate	Spoofing
MS16-010	No	CVE-2016-0029	Important	Spoofing
MS16-010	No	CVE-2016-0030	Important	Spoofing
MS16-010	No	CVE-2016-0031	Important	Spoofing
MS16-010	No	CVE-2016-0032	Important	Spoofing
MS16-011	Yes	CVE-2016-0060	Critical	Remote Code Execution
MS16-011	Yes	CVE-2016-0061	Critical	Remote Code Execution
MS16-011	Yes	CVE-2016-0062	Critical	Remote Code Execution
MS16-011	Yes	CVE-2016-0077	Moderate	Spoofing
MS16-011	Yes	CVE-2016-0080	Important	Security Feature Bypass
MS16-011	Yes	CVE-2016-0084	Critical	Remote Code Execution
MS16-012	Yes	CVE-2016-0058	Critical	Remote Code Execution
MS16-012	Yes	CVE-2016-0046	Critical	Remote Code Execution
MS16-013	Yes	CVE-2016-0038	Critical	Remote Code Execution
MS16-014	No	CVE-2016-0040	Important	Elevation of Privilege
MS16-014	No	CVE-2016-0041	Important	Remote Code Execution
MS16-014	No	CVE-2016-0042	Important	Remote Code Execution
MS16-014	No	CVE-2016-0044	Important	Denial of Service
MS16-014	No	CVE-2016-0049	Important	Security Feature Bypass
MS16-015	Yes	CVE-2016-0022	Critical	Remote Code Execution
MS16-015	Yes	CVE-2016-0052	Critical	Remote Code Execution
MS16-015	Yes	CVE-2016-0053	Critical	Remote Code Execution
MS16-015	Yes	CVE-2016-0054	Important	Remote Code Execution
MS16-015	Yes	CVE-2016-0055	Important	Remote Code Execution
MS16-015	Yes	CVE-2016-0056	Important	Remote Code Execution
MS16-016	No	CVE-2016-0051	Important	Elevation of Privilege
MS16-017	No	CVE-2016-0036	Important	Elevation of Privilege
MS16-018	No	CVE-2016-0048	Important	Elevation of Privilege
MS16-019	No	CVE-2016-0033	Important	Denial of Service
MS16-019	No	CVE-2016-0047	Important	Information Disclosure
MS16-020	No	CVE-2016-0037	Important	Denial of Service
MS16-021	No	CVE-2016-0050	Important	Denial of Service
MS16-022	No	CVE-2016-0964	Critical	Remote Code Execution
MS16-022	No	CVE-2016-0965	Critical	Remote Code Execution
MS16-022	No	CVE-2016-0966	Critical	Remote Code Execution
MS16-022	No	CVE-2016-0967	Critical	Remote Code Execution
MS16-022	No	CVE-2016-0968	Critical	Remote Code Execution
MS16-022	No	CVE-2016-0969	Critical	Remote Code Execution
MS16-022	No	CVE-2016-0970	Critical	Remote Code Execution
MS16-022	No	CVE-2016-0971	Critical	Remote Code Execution

Bulletin	Mitigated	Vulnerability	Severity Rating	Impact
MS16-022	No	CVE-2016-0972	Critical	Remote Code Execution
MS16-022	No	CVE-2016-0973	Critical	Remote Code Execution
MS16-022	No	CVE-2016-0974	Critical	Remote Code Execution
MS16-022	No	CVE-2016-0975	Critical	Remote Code Execution
MS16-022	No	CVE-2016-0976	Critical	Remote Code Execution
MS16-022	No	CVE-2016-0977	Critical	Remote Code Execution
MS16-022	No	CVE-2016-0978	Critical	Remote Code Execution
MS16-022	No	CVE-2016-0979	Critical	Remote Code Execution
MS16-022	No	CVE-2016-0980	Critical	Remote Code Execution
MS16-022	No	CVE-2016-0981	Critical	Remote Code Execution
MS16-022	No	CVE-2016-0982	Critical	Remote Code Execution
MS16-022	No	CVE-2016-0983	Critical	Remote Code Execution
MS16-022	No	CVE-2016-0984	Critical	Remote Code Execution
MS16-022	No	CVE-2016-0985	Critical	Remote Code Execution
MS16-023	Yes	CVE-2016-0102	Critical	Remote Code Execution
MS16-023	Yes	CVE-2016-0103	Critical	Remote Code Execution
MS16-023	Yes	CVE-2016-0104	Critical	Remote Code Execution
MS16-023	Yes	CVE-2016-0105	Critical	Remote Code Execution
MS16-023	Yes	CVE-2016-0106	Critical	Remote Code Execution
MS16-023	Yes	CVE-2016-0107	Critical	Remote Code Execution
MS16-023	Yes	CVE-2016-0108	Critical	Remote Code Execution
MS16-023	Yes	CVE-2016-0109	Critical	Remote Code Execution
MS16-023	Yes	CVE-2016-0110	Critical	Remote Code Execution
MS16-023	Yes	CVE-2016-0111	Critical	Remote Code Execution
MS16-023	Yes	CVE-2016-0112	Critical	Remote Code Execution
MS16-023	Yes	CVE-2016-0113	Critical	Remote Code Execution
MS16-023	Yes	CVE-2016-0114	Critical	Remote Code Execution
MS16-024	Yes	CVE-2016-0102	Critical	Remote Code Execution
MS16-024	Yes	CVE-2016-0105	Critical	Remote Code Execution
MS16-024	Yes	CVE-2016-0109	Critical	Remote Code Execution
MS16-024	Yes	CVE-2016-0110	Critical	Remote Code Execution
MS16-024	Yes	CVE-2016-0111	Critical	Remote Code Execution
MS16-024	Yes	CVE-2016-0116	Critical	Remote Code Execution
MS16-024	Yes	CVE-2016-0123	Critical	Remote Code Execution
MS16-024	Yes	CVE-2016-0124	Critical	Remote Code Execution
MS16-024	Yes	CVE-2016-0125	Moderate	Information Disclosure
MS16-024	Yes	CVE-2016-0129	Critical	Remote Code Execution
MS16-024	Yes	CVE-2016-0130	Critical	Remote Code Execution
MS16-025	No	CVE-2016-0100	Important	Remote Code Execution
MS16-026	No	CVE-2016-0120	Moderate	Denial of Service
MS16-026	No	CVE-2016-0121	Critical	Remote Code Execution
MS16-027	No	CVE-2016-0101	Critical	Remote Code Execution
MS16-027	No	CVE-2016-0098	Critical	Remote Code Execution
MS16-028	Yes	CVE-2016-0117	Critical	Remote Code Execution
MS16-028	Yes	CVE-2016-0118	Critical	Remote Code Execution
MS16-029	Yes	CVE-2016-0021	Important	Remote Code Execution

Bulletin	Mitigated	Vulnerability	Severity Rating	Impact
MS16-029	Yes	CVE-2016-0057	Important	Security Feature Bypass
MS16-029	Yes	CVE-2016-0134	Important	Remote Code Execution
MS16-030	No	CVE-2016-0091	Important	Remote Code Execution
MS16-030	No	CVE-2016-0092	Important	Remote Code Execution
MS16-031	No	CVE-2016-0087	Important	Elevation of Privilege
MS16-032	No	CVE-2016-0099	Important	Elevation of Privilege
MS16-033	No	CVE-2016-0133	Important	Elevation of Privilege
MS16-034	No	CVE-2016-0093	Important	Elevation of Privilege
MS16-034	No	CVE-2016-0094	Important	Elevation of Privilege
MS16-034	No	CVE-2016-0095	Important	Elevation of Privilege
MS16-034	No	CVE-2016-0096	Important	Elevation of Privilege
MS16-035	No	CVE-2016-0132	Important	Security Feature Bypass
MS16-036	No	CVE-2015-8652	Critical	Remote Code Execution
MS16-036	No	CVE-2015-8655	Critical	Remote Code Execution
MS16-036	No	CVE-2015-8658	Critical	Remote Code Execution
MS16-036	No	CVE-2016-0960	Critical	Remote Code Execution
MS16-036	No	CVE-2016-0961	Critical	Remote Code Execution
MS16-036	No	CVE-2016-0962	Critical	Remote Code Execution
MS16-036	No	CVE-2016-0963	Critical	Remote Code Execution
MS16-036	No	CVE-2016-0986	Critical	Remote Code Execution
MS16-036	No	CVE-2016-0987	Critical	Remote Code Execution
MS16-036	No	CVE-2016-0988	Critical	Remote Code Execution
MS16-036	No	CVE-2016-0989	Critical	Remote Code Execution
MS16-036	No	CVE-2016-0990	Critical	Remote Code Execution
MS16-036	No	CVE-2016-0991	Critical	Remote Code Execution
MS16-036	No	CVE-2016-0993	Critical	Remote Code Execution
MS16-036	No	CVE-2016-0994	Critical	Remote Code Execution
MS16-036	No	CVE-2016-0995	Critical	Remote Code Execution
MS16-036	No	CVE-2016-0996	Critical	Remote Code Execution
MS16-036	No	CVE-2016-1001	Critical	Remote Code Execution
MS16-036	No	CVE-2016-1005	Critical	Remote Code Execution
MS16-036	No	CVE-2016-1010	Critical	Remote Code Execution
MS16-037	Yes	CVE-2016-0154	Critical	Remote Code Execution
MS16-037	Yes	CVE-2016-0159	Critical	Remote Code Execution
MS16-037	Yes	CVE-2016-0160	Important	Remote Code Execution
MS16-037	Yes	CVE-2016-0162	Moderate	Information Disclosure
MS16-037	Yes	CVE-2016-0164	Critical	Remote Code Execution
MS16-037	Yes	CVE-2016-0166	Critical	Remote Code Execution
MS16-038	Yes	CVE-2016-0154	Critical	Remote Code Execution
MS16-038	Yes	CVE-2016-0155	Critical	Remote Code Execution
MS16-038	Yes	CVE-2016-0156	Critical	Remote Code Execution
MS16-038	Yes	CVE-2016-0157	Critical	Remote Code Execution
MS16-038	Yes	CVE-2016-0158	Important	Elevation of Privilege
MS16-038	Yes	CVE-2016-0161	Moderate	Elevation of Privilege
MS16-039	No	CVE-2016-0143	Important	Elevation of Privilege
MS16-039	No	CVE-2016-0145	Critical	Remote Code Execution

Bulletin	Mitigated	Vulnerability	Severity Rating	Impact
MS16-039	No	CVE-2016-0165	Important	Elevation of Privilege
MS16-039	No	CVE-2016-0167	Important	Elevation of Privilege
MS16-040	No	CVE-2016-0147	Critical	Remote Code Execution
MS16-041	No	CVE-2016-0148	Important	Remote Code Execution
MS16-042	Yes	CVE-2016-0122	Important	Remote Code Execution
MS16-042	Yes	CVE-2016-0127	Critical	Remote Code Execution
MS16-042	Yes	CVE-2016-0136	Important	Remote Code Execution
MS16-042	Yes	CVE-2016-0139	Important	Remote Code Execution
MS16-043	N/A			
MS16-044	No	CVE-2016-0153	Important	Remote Code Execution
MS16-045	No	CVE-2016-0088	Important	Remote Code Execution
MS16-045	No	CVE-2016-0089	Important	Information Disclosure
MS16-045	No	CVE-2016-0090	Important	Information Disclosure
MS16-046	No	CVE-2016-0135	Important	Elevation of Privilege
MS16-047	No	CVE-2016-0128	Important	Elevation of Privilege
MS16-048	No	CVE-2016-0151	Important	Security Feature Bypass
MS16-049	No	CVE-2016-0150	Important	Denial of Service
MS16-050	No	CVE-2016-1006	Critical	Remote Code Execution
MS16-050	No	CVE-2016-1011	Critical	Remote Code Execution
MS16-050	No	CVE-2016-1012	Critical	Remote Code Execution
MS16-050	No	CVE-2016-1013	Critical	Remote Code Execution
MS16-050	No	CVE-2016-1014	Critical	Remote Code Execution
MS16-050	No	CVE-2016-1015	Critical	Remote Code Execution
MS16-050	No	CVE-2016-1016	Critical	Remote Code Execution
MS16-050	No	CVE-2016-1017	Critical	Remote Code Execution
MS16-050	No	CVE-2016-1018	Critical	Remote Code Execution
MS16-050	No	CVE-2016-1019	Critical	Remote Code Execution
MS16-051	Yes	CVE-2016-0187	Critical	Remote Code Execution
MS16-051	Yes	CVE-2016-0188	Important	Security Feature Bypass
MS16-051	Yes	CVE-2016-0189	Critical	Remote Code Execution
MS16-051	Yes	CVE-2016-0192	Critical	Remote Code Execution
MS16-051	Yes	CVE-2016-0194	Important	Information Disclosure
MS16-052	Yes	CVE-2016-0186	Critical	Remote Code Execution
MS16-052	Yes	CVE-2016-0191	Critical	Remote Code Execution
MS16-052	Yes	CVE-2016-0192	Critical	Remote Code Execution
MS16-052	Yes	CVE-2016-0193	Critical	Remote Code Execution
MS16-053	Yes	CVE-2016-0187	Critical	Remote Code Execution
MS16-053	Yes	CVE-2016-0189	Critical	Remote Code Execution
MS16-054	Yes	CVE-2016-0126	Important	Remote Code Execution
MS16-054	Yes	CVE-2016-0140	Important	Remote Code Execution
MS16-054	Yes	CVE-2016-0183	Critical	Remote Code Execution
MS16-054	Yes	CVE-2016-0198	Critical	Remote Code Execution
MS16-055	Yes	CVE-2016-0168	Important	Information Disclosure
MS16-055	Yes	CVE-2016-0169	Important	Information Disclosure
MS16-055	Yes	CVE-2016-0170	Critical	Remote Code Execution
MS16-055	Yes	CVE-2016-0184	Critical	Remote Code Execution

Bulletin	Mitigated	Vulnerability	Severity Rating	Impact
MS16-055	Yes	CVE-2016-0195	Critical	Remote Code Execution
MS16-056	Yes	CVE-2016-0182	Critical	Remote Code Execution
MS16-057	Yes	CVE-2016-0179	Critical	Remote Code Execution
MS16-058	Yes	CVE-2016-0152	Important	Remote Code Execution
MS16-059	Yes	CVE-2016-0185	Important	Remote Code Execution
MS16-060	No	CVE-2016-0180	Important	Elevation of Privilege
MS16-061	No	CVE-2016-0178	Important	Remote Code Execution
MS16-062	No	CVE-2016-0171	Important	Elevation of Privilege
MS16-062	No	CVE-2016-0173	Important	Elevation of Privilege
MS16-062	No	CVE-2016-0174	Important	Elevation of Privilege
MS16-062	No	CVE-2016-0175	Important	Information Disclosure
MS16-062	No	CVE-2016-0176	Important	Elevation of Privilege
MS16-062	No	CVE-2016-0196	Important	Elevation of Privilege
MS16-062	No	CVE-2016-0197	Important	Elevation of Privilege
MS16-063	Yes	CVE-2016-0199	Critical	Remote Code Execution
MS16-063	Yes	CVE-2016-0200	Critical	Remote Code Execution
MS16-063	Yes	CVE-2016-3202	Critical	Remote Code Execution
MS16-063	Yes	CVE-2016-3205	Critical	Remote Code Execution
MS16-063	Yes	CVE-2016-3206	Critical	Remote Code Execution
MS16-063	Yes	CVE-2016-3207	Critical	Remote Code Execution
MS16-063	Yes	CVE-2016-3210	Critical	Remote Code Execution
MS16-063	Yes	CVE-2016-3211	Important	Remote Code Execution
MS16-063	Yes	CVE-2016-3212	Important	Remote Code Execution
MS16-063	Yes	CVE-2016-3213	Important	Elevation of Privilege
MS16-064	No	CVE-2016-1096	Critical	Remote Code Execution
MS16-064	No	CVE-2016-1097	Critical	Remote Code Execution
MS16-064	No	CVE-2016-1098	Critical	Remote Code Execution
MS16-064	No	CVE-2016-1099	Critical	Remote Code Execution
MS16-064	No	CVE-2016-1100	Critical	Remote Code Execution
MS16-064	No	CVE-2016-1101	Critical	Remote Code Execution
MS16-064	No	CVE-2016-1102	Critical	Remote Code Execution
MS16-064	No	CVE-2016-1103	Critical	Remote Code Execution
MS16-064	No	CVE-2016-1104	Critical	Remote Code Execution
MS16-064	No	CVE-2016-1105	Critical	Remote Code Execution
MS16-064	No	CVE-2016-1106	Critical	Remote Code Execution
MS16-064	No	CVE-2016-1107	Critical	Remote Code Execution
MS16-064	No	CVE-2016-1108	Critical	Remote Code Execution
MS16-064	No	CVE-2016-1109	Critical	Remote Code Execution
MS16-064	No	CVE-2016-1110	Critical	Remote Code Execution
MS16-064	No	CVE-2016-4108	Critical	Remote Code Execution
MS16-064	No	CVE-2016-4109	Critical	Remote Code Execution
MS16-064	No	CVE-2016-4110	Critical	Remote Code Execution
MS16-064	No	CVE-2016-4111	Critical	Remote Code Execution
MS16-064	No	CVE-2016-4112	Critical	Remote Code Execution
MS16-064	No	CVE-2016-4113	Critical	Remote Code Execution
MS16-064	No	CVE-2016-4114	Critical	Remote Code Execution

Bulletin	Mitigated	Vulnerability	Severity Rating	Impact
MS16-064	No	CVE-2016-4115	Critical	Remote Code Execution
MS16-064	No	CVE-2016-4116	Critical	Remote Code Execution
MS16-064	No	CVE-2016-4117	Critical	Remote Code Execution
MS16-065	No	CVE-2016-0149	Important	Information Disclosure
MS16-066	No	CVE-2016-0181	Important	Security Feature Bypass
MS16-067	No	CVE-2016-0190	Important	Information Disclosure
MS16-068	Yes	CVE-2016-3198	Important	Security Feature Bypass
MS16-068	Yes	CVE-2016-3199	Critical	Remote Code Execution
MS16-068	Yes	CVE-2016-3201	Important	Information Disclosure
MS16-068	Yes	CVE-2016-3202	Critical	Remote Code Execution
MS16-068	Yes	CVE-2016-3203	Critical	Remote Code Execution
MS16-068	Yes	CVE-2016-3214	Critical	Remote Code Execution
MS16-068	Yes	CVE-2016-3215	Important	Information Disclosure
MS16-068	Yes	CVE-2016-3222	Critical	Remote Code Execution
MS16-069	Yes	CVE-2016-3205	Critical	Remote Code Execution
MS16-069	Yes	CVE-2016-3206	Critical	Remote Code Execution
MS16-069	Yes	CVE-2016-3207	Critical	Remote Code Execution
MS16-070	Yes	CVE-2016-0025	Critical	Remote Code Execution
MS16-070	Yes	CVE-2016-3233	Important	Remote Code Execution
MS16-070	Yes	CVE-2016-3234	Important	Information Disclosure
MS16-070	Yes	CVE-2016-3235	Important	Remote Code Execution
MS16-071	No	CVE-2016-3227	Critical	Remote Code Execution
MS16-072	No	CVE-2016-3223	Important	Elevation of Privilege
MS16-073	No	CVE-2016-3218	Important	Elevation of Privilege
MS16-073	No	CVE-2016-3221	Important	Elevation of Privilege
MS16-073	No	CVE-2016-3232	Important	Information Disclosure
MS16-074	No	CVE-2016-3216	Important	Information Disclosure
MS16-074	No	CVE-2016-3219	Important	Elevation of Privilege
MS16-074	No	CVE-2016-3220	Important	Elevation of Privilege
MS16-075	No	CVE-2016-3225	Important	Elevation of Privilege
MS16-076	No	CVE-2016-3228	Important	Remote Code Execution
MS16-077	No	CVE-2016-3213	Important	Elevation of Privilege
MS16-077	No	CVE-2016-3236	Important	Elevation of Privilege
MS16-077	No	CVE-2016-3299	Important	Elevation of Privilege
MS16-078	No	CVE-2016-3231	Important	Elevation of Privilege
MS16-079	No	CVE-2016-0028	Important	Information Disclosure
MS16-079	No	CVE-2015-6013	Important	Elevation of Privilege
MS16-079	No	CVE-2015-6014	Important	Elevation of Privilege
MS16-079	No	CVE-2015-6015	Important	Elevation of Privilege
MS16-080	No	CVE-2016-3201	Important	Information Disclosure
MS16-080	No	CVE-2016-3203	Important	Remote Code Execution
MS16-080	No	CVE-2016-3215	Important	Information Disclosure
MS16-081	No	CVE-2016-3226	Important	Denial of Service
MS16-082	No	CVE-2016-3230	Important	Denial of Service
MS16-083	No	CVE-2016-4121	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4122	Critical	Remote Code Execution

Bulletin	Mitigated	Vulnerability	Severity Rating	Impact
MS16-083	No	CVE-2016-4123	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4124	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4125	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4126	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4127	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4128	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4129	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4130	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4131	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4132	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4133	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4134	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4135	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4136	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4137	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4138	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4139	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4140	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4141	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4142	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4143	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4144	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4145	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4146	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4147	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4148	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4149	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4150	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4151	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4152	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4153	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4154	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4155	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4156	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4166	Critical	Remote Code Execution
MS16-083	No	CVE-2016-4171	Critical	Remote Code Execution
MS16-084	Yes	CVE-2016-3204	Critical	Remote Code Execution
MS16-084	Yes	CVE-2016-3240	Critical	Remote Code Execution
MS16-084	Yes	CVE-2016-3241	Critical	Remote Code Execution
MS16-084	Yes	CVE-2016-3242	Critical	Remote Code Execution
MS16-084	Yes	CVE-2016-3243	Important	Remote Code Execution
MS16-084	Yes	CVE-2016-3245	Moderate	Security Feature Bypass
MS16-084	Yes	CVE-2016-3248	Critical	Remote Code Execution
MS16-084	Yes	CVE-2016-3259	Critical	Remote Code Execution
MS16-084	Yes	CVE-2016-3260	Critical	Remote Code Execution
MS16-084	Yes	CVE-2016-3261	Important	Information Disclosure

Bulletin	Mitigated	Vulnerability	Severity Rating	Impact
MS16-084	Yes	CVE-2016-3264	Critical	Remote Code Execution
MS16-084	Yes	CVE-2016-3273	Important	Information Disclosure
MS16-084	Yes	CVE-2016-3274	Moderate	Spoofing
MS16-084	Yes	CVE-2016-3276	Important	Spoofing
MS16-084	Yes	CVE-2016-3277	Important	Information Disclosure
MS16-085	Yes	CVE-2016-3244	Important	Security Feature Bypass
MS16-085	Yes	CVE-2016-3246	Critical	Remote Code Execution
MS16-085	Yes	CVE-2016-3248	Critical	Remote Code Execution
MS16-085	Yes	CVE-2016-3259	Critical	Remote Code Execution
MS16-085	Yes	CVE-2016-3260	Critical	Remote Code Execution
MS16-085	Yes	CVE-2016-3264	Critical	Remote Code Execution
MS16-085	Yes	CVE-2016-3265	Critical	Remote Code Execution
MS16-085	Yes	CVE-2016-3269	Critical	Remote Code Execution
MS16-085	Yes	CVE-2016-3271	Important	Information Disclosure
MS16-085	Yes	CVE-2016-3273	Important	Information Disclosure
MS16-085	Yes	CVE-2016-3274	Important	Spoofing
MS16-085	Yes	CVE-2016-3276	Important	Spoofing
MS16-085	Yes	CVE-2016-3277	Important	Information Disclosure
MS16-086	Yes	CVE-2016-3204	Critical	Remote Code Execution
MS16-087	No	CVE-2016-3238	Critical	Remote Code Execution
MS16-087	No	CVE-2016-3239	Important	Elevation of Privilege
MS16-088	Yes	CVE-2016-3278	Important	Remote Code Execution
MS16-088	Yes	CVE-2016-3279	Important	Security Feature Bypass
MS16-088	Yes	CVE-2016-3280	Critical	Remote Code Execution
MS16-088	Yes	CVE-2016-3281	Critical	Remote Code Execution
MS16-088	Yes	CVE-2016-3282	Critical	Remote Code Execution
MS16-088	Yes	CVE-2016-3283	Critical	Remote Code Execution
MS16-088	Yes	CVE-2016-3284	Important	Remote Code Execution
MS16-089	No	CVE-2016-3256	Important	Information Disclosure
MS16-090	No	CVE-2016-3249	Important	Elevation of Privilege
MS16-090	No	CVE-2016-3250	Important	Elevation of Privilege
MS16-090	No	CVE-2016-3251	Important	Information Disclosure
MS16-090	No	CVE-2016-3252	Important	Elevation of Privilege
MS16-090	No	CVE-2016-3254	Important	Elevation of Privilege
MS16-090	No	CVE-2016-3286	Important	Elevation of Privilege
MS16-091	No	CVE-2016-3255	Important	Information Disclosure
MS16-092	No	CVE-2016-3258	Important	Security Feature Bypass
MS16-092	No	CVE-2016-3272	Important	Information Disclosure
MS16-093	No	CVE-2016-4173	Critical	Remote Code Execution
MS16-093	No	CVE-2016-4174	Critical	Remote Code Execution
MS16-093	No	CVE-2016-4175	Critical	Remote Code Execution
MS16-093	No	CVE-2016-4176	Critical	Remote Code Execution
MS16-093	No	CVE-2016-4177	Critical	Remote Code Execution
MS16-093	No	CVE-2016-4178	Critical	Remote Code Execution
MS16-093	No	CVE-2016-4179	Critical	Remote Code Execution
MS16-093	No	CVE-2016-4182	Critical	Remote Code Execution

Bulletin	Mitigated	Vulnerability	Severity Rating	Impact
MS16-093	No	CVE-2016-4188	Critical	Remote Code Execution
MS16-093	No	CVE-2016-4185	Critical	Remote Code Execution
MS16-093	No	CVE-2016-4222	Critical	Remote Code Execution
MS16-093	No	CVE-2016-4223	Critical	Remote Code Execution
MS16-093	No	CVE-2016-4224	Critical	Remote Code Execution
MS16-093	No	CVE-2016-4225	Critical	Remote Code Execution
MS16-093	No	CVE-2016-4226	Critical	Remote Code Execution
MS16-093	No	CVE-2016-4227	Critical	Remote Code Execution
MS16-093	No	CVE-2016-4228	Critical	Remote Code Execution
MS16-093	No	CVE-2016-4229	Critical	Remote Code Execution
MS16-093	No	CVE-2016-4230	Critical	Remote Code Execution
MS16-093	No	CVE-2016-4231	Critical	Remote Code Execution
MS16-093	No	CVE-2016-4232	Critical	Remote Code Execution
MS16-093	No	CVE-2016-4247	Critical	Remote Code Execution
MS16-093	No	CVE-2016-4248	Critical	Remote Code Execution
MS16-093	No	CVE-2016-4249	Critical	Remote Code Execution
MS16-094	No	CVE-2016-3287	Important	Security Feature Bypass
MS16-095	Yes	CVE-2016-3288	Critical	Remote Code Execution
MS16-095	Yes	CVE-2016-3289	Critical	Remote Code Execution
MS16-095	Yes	CVE-2016-3290	Critical	Remote Code Execution
MS16-095	Yes	CVE-2016-3293	Critical	Remote Code Execution
MS16-095	Yes	CVE-2016-3321	Moderate	Information Disclosure
MS16-095	Yes	CVE-2016-3322	Critical	Remote Code Execution
MS16-095	Yes	CVE-2016-3326	Important	Information Disclosure
MS16-095	Yes	CVE-2016-3327	Important	Information Disclosure
MS16-095	Yes	CVE-2016-3329	Moderate	Information Disclosure
MS16-096	Yes	CVE-2016-3289	Critical	Remote Code Execution
MS16-096	Yes	CVE-2016-3293	Important	Remote Code Execution
MS16-096	Yes	CVE-2016-3296	Critical	Remote Code Execution
MS16-096	Yes	CVE-2016-3319	Critical	Remote Code Execution
MS16-096	Yes	CVE-2016-3322	Critical	Remote Code Execution
MS16-096	Yes	CVE-2016-3326	Important	Information Disclosure
MS16-096	Yes	CVE-2016-3327	Important	Information Disclosure
MS16-096	Yes	CVE-2016-3329	Moderate	Information Disclosure
MS16-097	Yes	CVE-2016-3301	Critical	Remote Code Execution
MS16-097	Yes	CVE-2016-3303	Critical	Remote Code Execution
MS16-097	Yes	CVE-2016-3304	Critical	Remote Code Execution
MS16-098	No	CVE-2016-3308	Important	Elevation of Privilege
MS16-098	No	CVE-2016-3309	Important	Elevation of Privilege
MS16-098	No	CVE-2016-3310	Important	Elevation of Privilege
MS16-098	No	CVE-2016-3311	Important	Elevation of Privilege
MS16-099	Yes	CVE-2016-3313	Important	Remote Code Execution
MS16-099	Yes	CVE-2016-3315	Important	Information Disclosure
MS16-099	Yes	CVE-2016-3316	Critical	Remote Code Execution
MS16-099	Yes	CVE-2016-3317	Important	Remote Code Execution
MS16-099	Yes	CVE-2016-3318	Important	Remote Code Execution

Bulletin	Mitigated	Vulnerability	Severity Rating	Impact
MS16-100	No	CVE-2016-3320	Important	Security Feature Bypass
MS16-101	No	CVE-2016-3237	Important	Security Feature Bypass
MS16-101	No	CVE-2016-3300	Important	Elevation of Privilege
MS16-102	Yes	CVE-2016-3319	Critical	Remote Code Execution
MS16-103	No	CVE-2016-3312	Important	Information Disclosure
MS16-104	Yes	CVE-2016-3247	Important	Remote Code Execution
MS16-104	Yes	CVE-2016-3291	Moderate	Information Disclosure
MS16-104	Yes	CVE-2016-3292	Important	Elevation of Privilege
MS16-104	Yes	CVE-2016-3295	Critical	Remote Code Execution
MS16-104	Yes	CVE-2016-3297	Important	Remote Code Execution
MS16-104	Yes	CVE-2016-3324	Important	Remote Code Execution
MS16-104	Yes	CVE-2016-3325	Important	Information Disclosure
MS16-104	Yes	CVE-2016-3351	Important	Information Disclosure
MS16-104	Yes	CVE-2016-3353	Important	Security Feature Bypass
MS16-104	Yes	CVE-2016-3375	Critical	Remote Code Execution
MS16-105	Yes	CVE-2016-3247	Important	Remote Code Execution
MS16-105	Yes	CVE-2016-3291	Moderate	Information Disclosure
MS16-105	Yes	CVE-2016-3294	Critical	Remote Code Execution
MS16-105	Yes	CVE-2016-3295	Critical	Remote Code Execution
MS16-105	Yes	CVE-2016-3297	Important	Remote Code Execution
MS16-105	Yes	CVE-2016-3325	Important	Information Disclosure
MS16-105	Yes	CVE-2016-3330	Important	Remote Code Execution
MS16-105	Yes	CVE-2016-3350	Critical	Remote Code Execution
MS16-105	Yes	CVE-2016-3351	Important	Information Disclosure
MS16-105	Yes	CVE-2016-3370	Important	Information Disclosure
MS16-105	Yes	CVE-2016-3374	Important	Information Disclosure
MS16-105	Yes	CVE-2016-3377	Critical	Remote Code Execution
MS16-106	Yes	CVE-2016-3348	Important	Elevation of Privilege
MS16-106	Yes	CVE-2016-3349	Important	Elevation of Privilege
MS16-106	Yes	CVE-2016-3354	Important	Information Disclosure
MS16-106	Yes	CVE-2016-3355	Important	Elevation of Privilege
MS16-106	Yes	CVE-2016-3356	Critical	Remote Code Execution
MS16-107	Yes	CVE-2016-0137	Important	Security Feature Bypass
MS16-107	Yes	CVE-2016-0141	Important	Information Disclosure
MS16-107	Yes	CVE-2016-3357	Critical	Remote Code Execution
MS16-107	Yes	CVE-2016-3358	Important	Remote Code Execution
MS16-107	Yes	CVE-2016-3359	Important	Remote Code Execution
MS16-107	Yes	CVE-2016-3360	Important	Remote Code Execution
MS16-107	Yes	CVE-2016-3361	Important	Remote Code Execution
MS16-107	Yes	CVE-2016-3362	Important	Remote Code Execution
MS16-107	Yes	CVE-2016-3363	Important	Remote Code Execution
MS16-107	Yes	CVE-2016-3364	Important	Remote Code Execution
MS16-107	Yes	CVE-2016-3365	Important	Remote Code Execution
MS16-107	Yes	CVE-2016-3366	Important	Remote Code Execution
MS16-107	Yes	CVE-2016-3381	Important	Remote Code Execution
MS16-108	No	CVE-2016-0138	Important	Information Disclosure

Bulletin	Mitigated	Vulnerability	Severity Rating	Impact
MS16-108	No	CVE-2016-3378	Moderate	Spoofing
MS16-108	No	CVE-2016-3379	Important	Elevation of Privilege
MS16-108	No	CVE-2016-3575	Critical	Remote Code Execution
MS16-108	No	CVE-2016-3581	Critical	Remote Code Execution
MS16-108	No	CVE-2016-3582	Critical	Remote Code Execution
MS16-108	No	CVE-2016-3583	Critical	Remote Code Execution
MS16-108	No	CVE-2016-3595	Critical	Remote Code Execution
MS16-108	No	CVE-2016-3594	Critical	Remote Code Execution
MS16-108	No	CVE-2015-6014	Critical	Remote Code Execution
MS16-108	No	CVE-2016-3593	Critical	Remote Code Execution
MS16-108	No	CVE-2016-3592	Critical	Remote Code Execution
MS16-108	No	CVE-2016-3596	Critical	Remote Code Execution
MS16-108	No	CVE-2016-3591	Critical	Remote Code Execution
MS16-108	No	CVE-2016-3574	Critical	Information Disclosure
MS16-108	No	CVE-2016-3576	Critical	Denial of Service
MS16-108	No	CVE-2016-3577	Critical	Denial of Service
MS16-108	No	CVE-2016-3578	Critical	Denial of Service
MS16-108	No	CVE-2016-3579	Critical	Denial of Service
MS16-108	No	CVE-2016-3580	Critical	Denial of Service
MS16-108	No	CVE-2016-3590	Critical	Denial of Service
MS16-109	No	CVE-2016-3367	Important	Remote Code Execution
MS16-110	No	CVE-2016-3346	Important	Elevation of Privilege
MS16-110	No	CVE-2016-3352	Important	Information Disclosure
MS16-110	No	CVE-2016-3368	Important	Remote Code Execution
MS16-110	No	CVE-2016-3369	Important	Denial of Service
MS16-111	No	CVE-2016-3305	Important	Elevation of Privilege
MS16-111	No	CVE-2016-3306	Important	Elevation of Privilege
MS16-111	No	CVE-2016-3371	Important	Elevation of Privilege
MS16-111	No	CVE-2016-3372	Important	Elevation of Privilege
MS16-111	No	CVE-2016-3373	Important	Elevation of Privilege
MS16-112	No	CVE-2016-3302	Important	Elevation of Privilege
MS16-113	No	CVE-2016-3344	Important	Information Disclosure
MS16-114	No	CVE-2016-3345	Important	Remote Code Execution
MS16-115	No	CVE-2016-3370	Important	Information Disclosure
MS16-115	No	CVE-2016-3374	Important	Information Disclosure
MS16-116	No	CVE-2016-3375	Critical	Remote Code Execution
MS16-117	No	CVE-2016-4271	Critical	Remote Code Execution
MS16-117	No	CVE-2016-4272	Critical	Remote Code Execution
MS16-117	No	CVE-2016-4274	Critical	Remote Code Execution
MS16-117	No	CVE-2016-4275	Critical	Remote Code Execution
MS16-117	No	CVE-2016-4276	Critical	Remote Code Execution
MS16-117	No	CVE-2016-4277	Critical	Remote Code Execution
MS16-117	No	CVE-2016-4278	Critical	Remote Code Execution
MS16-117	No	CVE-2016-4279	Critical	Remote Code Execution
MS16-117	No	CVE-2016-4280	Critical	Remote Code Execution
MS16-117	No	CVE-2016-4281	Critical	Remote Code Execution

Bulletin	Mitigated	Vulnerability	Severity Rating	Impact
MS16-117	No	CVE-2016-4282	Critical	Remote Code Execution
MS16-117	No	CVE-2016-4283	Critical	Remote Code Execution
MS16-117	No	CVE-2016-4284	Critical	Remote Code Execution
MS16-117	No	CVE-2016-4285	Critical	Remote Code Execution
MS16-117	No	CVE-2016-4287	Critical	Remote Code Execution
MS16-117	No	CVE-2016-6921	Critical	Remote Code Execution
MS16-117	No	CVE-2016-6922	Critical	Remote Code Execution
MS16-117	No	CVE-2016-6923	Critical	Remote Code Execution
MS16-117	No	CVE-2016-6924	Critical	Remote Code Execution
MS16-117	No	CVE-2016-6925	Critical	Remote Code Execution
MS16-117	No	CVE-2016-6926	Critical	Remote Code Execution
MS16-117	No	CVE-2016-6927	Critical	Remote Code Execution
MS16-117	No	CVE-2016-6929	Critical	Remote Code Execution
MS16-117	No	CVE-2016-6930	Critical	Remote Code Execution
MS16-117	No	CVE-2016-6931	Critical	Remote Code Execution
MS16-117	No	CVE-2016-6932	Critical	Remote Code Execution
MS16-118	Yes	CVE-2016-3267	Moderate	Information Disclosure
MS16-118	Yes	CVE-2016-3298	Moderate	Information Disclosure
MS16-118	Yes	CVE-2016-3331	Critical	Remote Code Execution
MS16-118	Yes	CVE-2016-3382	Critical	Remote Code Execution
MS16-118	Yes	CVE-2016-3383	Critical	Remote Code Execution
MS16-118	Yes	CVE-2016-3384	Critical	Remote Code Execution
MS16-118	Yes	CVE-2016-3385	Critical	Remote Code Execution
MS16-118	Yes	CVE-2016-3387	Important	Elevation of Privilege
MS16-118	Yes	CVE-2016-3388	Important	Elevation of Privilege
MS16-118	Yes	CVE-2016-3390	Important	Remote Code Execution
MS16-118	Yes	CVE-2016-3391	Moderate	Information Disclosure
MS16-119	Yes	CVE-2016-3267	Moderate	Information Disclosure
MS16-119	Yes	CVE-2016-3331	Critical	Remote Code Execution
MS16-119	Yes	CVE-2016-3382	Critical	Remote Code Execution
MS16-119	Yes	CVE-2016-3386	Critical	Remote Code Execution
MS16-119	Yes	CVE-2016-3387	Important	Elevation of Privilege
MS16-119	Yes	CVE-2016-3388	Important	Elevation of Privilege
MS16-119	Yes	CVE-2016-3389	Critical	Remote Code Execution
MS16-119	Yes	CVE-2016-3390	Critical	Remote Code Execution
MS16-119	Yes	CVE-2016-3391	Moderate	Information Disclosure
MS16-119	Yes	CVE-2016-3392	Critical	Security Feature Bypass
MS16-119	Yes	CVE-2016-7189	Critical	Remote Code Execution
MS16-119	Yes	CVE-2016-7190	Critical	Remote Code Execution
MS16-119	Yes	CVE-2016-7194	Critical	Remote Code Execution
MS16-120	Yes	CVE-2016-3209	Important	Information Disclosure
MS16-120	Yes	CVE-2016-3262	Important	Information Disclosure
MS16-120	Yes	CVE-2016-3263	Important	Information Disclosure
MS16-120	Yes	CVE-2016-3270	Important	Elevation of Privilege
MS16-120	Yes	CVE-2016-3393	Critical	Remote Code Execution
MS16-120	Yes	CVE-2016-3396	Critical	Remote Code Execution

Bulletin	Mitigated	Vulnerability	Severity Rating	Impact
MS16-120	Yes	CVE-2016-7182	Important	Elevation of Privilege
MS16-121	No	CVE-2016-7193	Critical	Remote Code Execution
MS16-122	Yes	CVE-2016-0142	Critical	Remote Code Execution
MS16-123	No	CVE-2016-3266	Important	Elevation of Privilege
MS16-123	No	CVE-2016-3341	Important	Elevation of Privilege
MS16-123	No	CVE-2016-3376	Important	Elevation of Privilege
MS16-123	No	CVE-2016-7185	Important	Elevation of Privilege
MS16-123	No	CVE-2016-7211	Important	Elevation of Privilege
MS16-124	No	CVE-2016-0070	Important	Elevation of Privilege
MS16-124	No	CVE-2016-0073	Important	Elevation of Privilege
MS16-124	No	CVE-2016-0075	Important	Elevation of Privilege
MS16-124	No	CVE-2016-0079	Important	Elevation of Privilege
MS16-125	No	CVE-2016-7188	Important	Elevation of Privilege
MS16-126	No	CVE-2016-3298	Moderate	Information Disclosure
MS16-127	No	CVE-2016-4273	Critical	Remote Code Execution
MS16-127	No	CVE-2016-4286	Critical	Remote Code Execution
MS16-127	No	CVE-2016-6981	Critical	Remote Code Execution
MS16-127	No	CVE-2016-6982	Critical	Remote Code Execution
MS16-127	No	CVE-2016-6983	Critical	Remote Code Execution
MS16-127	No	CVE-2016-6984	Critical	Remote Code Execution
MS16-127	No	CVE-2016-6985	Critical	Remote Code Execution
MS16-127	No	CVE-2016-6986	Critical	Remote Code Execution
MS16-127	No	CVE-2016-6987	Critical	Remote Code Execution
MS16-127	No	CVE-2016-6989	Critical	Remote Code Execution
MS16-127	No	CVE-2016-6990	Critical	Remote Code Execution
MS16-127	No	CVE-2016-6992	Critical	Remote Code Execution
MS16-128	No	CVE-2016-7855	Critical	Remote Code Execution
MS16-129	Yes	CVE-2016-7195	Critical	Remote Code Execution
MS16-129	Yes	CVE-2016-7196	Critical	Remote Code Execution
MS16-129	Yes	CVE-2016-7198	Critical	Remote Code Execution
MS16-129	Yes	CVE-2016-7199	Moderate	Information Disclosure
MS16-129	Yes	CVE-2016-7200	Critical	Remote Code Execution
MS16-129	Yes	CVE-2016-7201	Critical	Remote Code Execution
MS16-129	Yes	CVE-2016-7202	Important	Remote Code Execution
MS16-129	Yes	CVE-2016-7203	Critical	Remote Code Execution
MS16-129	Yes	CVE-2016-7204	Important	Information Disclosure
MS16-129	Yes	CVE-2016-7208	Critical	Remote Code Execution
MS16-129	Yes	CVE-2016-7209	Moderate	Spoofing
MS16-129	Yes	CVE-2016-7227	Moderate	Information Disclosure
MS16-129	Yes	CVE-2016-7239	Moderate	Information Disclosure
MS16-129	Yes	CVE-2016-7240	Critical	Remote Code Execution
MS16-129	Yes	CVE-2016-7241	Critical	Remote Code Execution
MS16-129	Yes	CVE-2016-7242	Critical	Remote Code Execution
MS16-129	Yes	CVE-2016-7243	Critical	Remote Code Execution
MS16-130	No	CVE-2016-7221	Important	Elevation of Privilege
MS16-130	No	CVE-2016-7222	Important	Elevation of Privilege

Bulletin	Mitigated	Vulnerability	Severity Rating	Impact
MS16-130	No	CVE-2016-7212	Critical	Remote Code Execution
MS16-131	Yes	CVE-2016-7248	Critical	Remote Code Execution
MS16-132	Yes	CVE-2016-7210	Important	information Disclosure
MS16-132	Yes	CVE-2016-7205	Critical	Remote Code Execution
MS16-132	Yes	CVE-2016-7217	Important	Remote Code Execution
MS16-132	Yes	CVE-2016-7256	Critical	Remote Code Execution
MS16-133	Yes	CVE-2016-7213	Important	Remote Code Execution
MS16-133	Yes	CVE-2016-7228	Important	Remote Code Execution
MS16-133	Yes	CVE-2016-7229	Important	Remote Code Execution
MS16-133	Yes	CVE-2016-7230	Important	Remote Code Execution
MS16-133	Yes	CVE-2016-7231	Important	Remote Code Execution
MS16-133	Yes	CVE-2016-7232	Important	Remote Code Execution
MS16-134	No	CVE-2016-0026	Important	Elevation of Privilege
MS16-134	No	CVE-2016-3332	Important	Elevation of Privilege
MS16-134	No	CVE-2016-3333	Important	Elevation of Privilege
MS16-134	No	CVE-2016-3334	Important	Elevation of Privilege
MS16-134	No	CVE-2016-3335	Important	Elevation of Privilege
MS16-134	No	CVE-2016-3338	Important	Elevation of Privilege
MS16-134	No	CVE-2016-3340	Important	Elevation of Privilege
MS16-134	No	CVE-2016-3342	Important	Elevation of Privilege
MS16-134	No	CVE-2016-3343	Important	Elevation of Privilege
MS16-134	No	CVE-2016-7184	Important	Elevation of Privilege
MS16-135	No	CVE-2016-7214	Important	Information Disclosure
MS16-135	No	CVE-2016-7215	Important	Elevation of Privilege
MS16-135	No	CVE- 2016-7218	Important	Information Disclosure
MS16-135	No	CVE-2016-7246	Important	Elevation of Privilege
MS16-135	No	CVE-2016-7255	Important	Elevation of Privilege
MS16-136	No	CVE-2016-7249	Important	Elevation of Privilege
MS16-136	No	CVE-2016-7250	Important	Elevation of Privilege
MS16-136	No	CVE-2016-7254	Important	Elevation of Privilege
MS16-136	No	CVE-2016-7251	Important	Elevation of Privilege
MS16-136	No	CVE-2016-7252	Important	Information Disclosure
MS16-136	No	CVE-2016-7253	Important	Elevation of Privilege
MS16-137	No	CVE-2016-7220	Important	Information Disclosure
MS16-137	No	CVE-2016-7237	Important	Denial of Service
MS16-137	No	CVE-2016-7238	Important	Elevation of Privilege
MS16-138	No	CVE-2016-7223	Important	Elevation of Privilege
MS16-138	No	CVE-2016-7224	Important	Elevation of Privilege
MS16-138	No	CVE-2016-7225	Important	Elevation of Privilege
MS16-138	No	CVE-2016-7226	Important	Elevation of Privilege
MS16-139	No	CVE-2016-7216	Important	Elevation of Privilege
MS16-140	No	CVE-2016-7247	Important	Security Feature Bypass
MS16-141	No	CVE-2016-7857	Critical	Remote Code Execution
MS16-141	No	CVE-2016-7858	Critical	Remote Code Execution
MS16-141	No	CVE-2016-7859	Critical	Remote Code Execution
MS16-141	No	CVE-2016-7860	Critical	Remote Code Execution

Bulletin	Mitigated	Vulnerability	Severity Rating	Impact
MS16-141	No	CVE-2016-7861	Critical	Remote Code Execution
MS16-141	No	CVE-2016-7862	Critical	Remote Code Execution
MS16-141	No	CVE-2016-7863	Critical	Remote Code Execution
MS16-141	No	CVE-2016-7864	Critical	Remote Code Execution
MS16-141	No	CVE-2016-7865	Critical	Remote Code Execution
MS16-142	Yes	CVE-2016-7195	Critical	Remote Code Execution
MS16-142	Yes	CVE-2016-7196	Critical	Remote Code Execution
MS16-142	Yes	CVE-2016-7198	Critical	Remote Code Execution
MS16-142	Yes	CVE-2016-7199	Moderate	Information Disclosure
MS16-142	Yes	CVE-2016-7227	Important	Information Disclosure
MS16-142	Yes	CVE-2016-7239	Moderate	Information Disclosure
MS16-142	Yes	CVE-2016-7241	Critical	Remote Code Execution
MS16-143	N/A			
MS16-144	Yes	CVE-2016-7202	Critical	Remote Code Execution
MS16-144	Yes	CVE-2016-7278	Important	Information Disclosure
MS16-144	Yes	CVE-2016-7279	Important	Remote Code Execution
MS16-144	Yes	CVE-2016-7281	Important	Security Feature Bypass
MS16-144	Yes	CVE-2016-7282	Important	Information Disclosure
MS16-144	Yes	CVE-2016-7283	Critical	Remote Code Execution
MS16-144	Yes	CVE-2016-7284	Important	Information Disclosure
MS16-144	Yes	CVE-2016-7287	Critical	Remote Code Execution
MS16-145	Yes	CVE-2016-7181	Moderate	Remote Code Execution
MS16-145	Yes	CVE-2016-7206	Important	Information Disclosure
MS16-145	Yes	CVE-2016-7279	Important	Remote Code Execution
MS16-145	Yes	CVE-2016-7280	Important	Information Disclosure
MS16-145	Yes	CVE-2016-7281	Important	Information Disclosure
MS16-145	Yes	CVE-2016-7282	Important	Information Disclosure
MS16-145	Yes	CVE-2016-7286	Important	Remote Code Execution
MS16-145	Yes	CVE-2016-7287	Critical	Remote Code Execution
MS16-145	Yes	CVE-2016-7288	Critical	Remote Code Execution
MS16-145	Yes	CVE-2016-7296	Critical	Remote Code Execution
MS16-145	Yes	CVE-2016-7297	Critical	Remote Code Execution
MS16-146	Yes	CVE-2016-7257	Important	Information Disclosure
MS16-146	Yes	CVE-2016-7272	Critical	Remote Code Execution
MS16-146	Yes	CVE-2016-7273	Critical	Remote Code Execution
MS16-147	Yes	CVE-2016-7274	Critical	Remote Code Execution
MS16-148	Yes	CVE-2016-7262	Important	Remote Code Execution
MS16-148	Yes	CVE-2016-7264	Important	Information Disclosure
MS16-148	Yes	CVE-2016-7265	Important	Remote Code Execution
MS16-148	Yes	CVE-2016-7266	Important	Remote Code Execution
MS16-148	Yes	CVE-2016-7267	Moderate	Security Feature Bypass
MS16-148	Yes	CVE-2016-7268	Important	Information Disclosure
MS16-148	Yes	CVE-2016-7274	Critical	Remote Code Execution
MS16-148	Yes	CVE-2016-7275	Important	Remote Code Execution
MS16-148	Yes	CVE-2016-7276	Important	Information Disclosure
MS16-148	Yes	CVE-2016-7277	Important	Remote Code Execution

Bulletin	Mitigated	Vulnerability	Severity Rating	Impact
MS16-148	Yes	CVE-2016-7289	Important	Remote Code Execution
MS16-148	Yes	CVE-2016-7290	Important	Information Disclosure
MS16-148	Yes	CVE-2016-7291	Important	Information Disclosure
MS16-148	Yes	CVE-2016-7263	Important	Remote Code Execution
MS16-148	Yes	CVE-2016-7264	Important	Information Disclosure
MS16-148	Yes	CVE-2016-7266	Important	Remote Code Execution
MS16-148	Yes	CVE-2016-7268	Important	information Disclosure
MS16-148	Yes	CVE-2016-7300	Important	Elevation of Privilege
MS16-148	Yes	CVE-2016-7257	Important	Information Disclosure
MS16-148	Yes	CVE-2016-7290	Important	Information Disclosure
MS16-148	Yes	CVE-2016-7291	Important	Information Disclosure
MS16-148	Yes	CVE-2016-7274	Critical	Remote Code Execution
MS16-148	Yes	CVE-2016-7276	Important	Information Disclosure
MS16-148	Yes	CVE-2016-7265	Important	Information Disclosure
MS16-148	Yes	CVE-2016-7268	Important	Information Disclosure
MS16-148	Yes	CVE-2016-7290	Important	Information Disclosure
MS16-148	Yes	CVE-2016-7291	Important	Information Disclosure
MS16-149	No	CVE-2016-7219	Important	Elevation of Privilege
MS16-149	No	CVE-2016-7292	Important	Elevation of Privilege
MS16-150	No	CVE-2016-7271	Important	Elevation of Privilege
MS16-151	No	CVE-2016-7259	Important	Elevation of Privilege
MS16-151	No	CVE-2016-7260	Important	Elevation of Privilege
MS16-152	No	CVE-2016-7258	Important	Information Disclosure
MS16-153	No	CVE-2016-7295	Important	Information Disclosure
MS16-154	No	CVE-2016-7867	Critical	Remote Code Execution
MS16-154	No	CVE-2016-7868	Critical	Remote Code Execution
MS16-154	No	CVE-2016-7869	Critical	Remote Code Execution
MS16-154	No	CVE-2016-7870	Critical	Remote Code Execution
MS16-154	No	CVE-2016-7871	Critical	Remote Code Execution
MS16-154	No	CVE-2016-7872	Critical	Remote Code Execution
MS16-154	No	CVE-2016-7873	Critical	Remote Code Execution
MS16-154	No	CVE-2016-7874	Critical	Remote Code Execution
MS16-154	No	CVE-2016-7875	Critical	Remote Code Execution
MS16-154	No	CVE-2016-7876	Critical	Remote Code Execution
MS16-154	No	CVE-2016-7877	Critical	Remote Code Execution
MS16-154	No	CVE-2016-7878	Critical	Remote Code Execution
MS16-154	No	CVE-2016-7879	Critical	Remote Code Execution
MS16-154	No	CVE-2016-7880	Critical	Remote Code Execution
MS16-154	No	CVE-2016-7881	Critical	Remote Code Execution
MS16-154	No	CVE-2016-7890	Critical	Remote Code Execution
MS16-154	No	CVE-2016-7892	Critical	Remote Code Execution
MS16-155	No	CVE-2016-7270	Important	Information Disclosure