Advanced Notification of Microsoft Security Update Release – April 2017

Security Advisory AE-Advisory 17-19

Criticality Critical

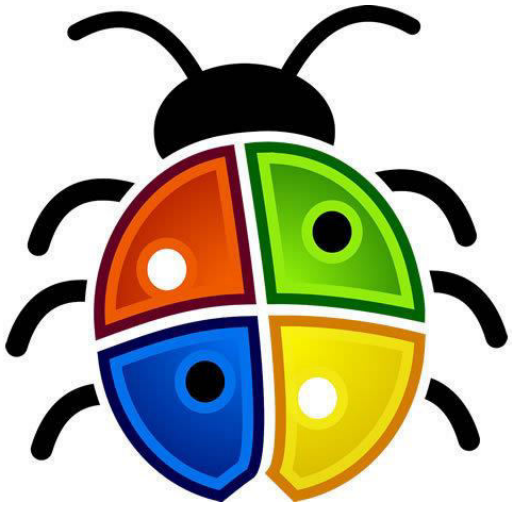
Advisory Released On 12 April 2017

Purpose

To provide an overview of the latest security updates released by Microsoft on 12 April, 2017.

Summary

aeCERT has received the latest Microsoft Security Update Release for April 2017. The Microsoft Security Response Center releases security bulletins on a monthly basis addressing security vulnerabilities in Microsoft software, describing their remediation, and providing links to the applicable updates for affected software. Each security bulletin is accompanied by one or more unique Knowledge Base Articles to provide further information about the updates. Refer to the “Advisory Details” section below for furhter information.



Advisory Details

Security update release overview

Product Family	Maximum Severity	Maximum Impact	Restart Required?	Associated KB Articles and/or Support Webpages
Windows 10 and Windows Server 2016 (including Microsoft Edge)	Critical	Remote Code Execution	Requires restart	Windows 10 RTM: KB4015221; Windows 10 1511: KB4015219; Windows 10 1607: KB4015217; Windows 10 1703: KB4015583; Windows Server 2016: KB4015217.
Windows 8.1 and Windows Server 2012 R2	Critical	Remote Code Execution	Requires restart	Windows 8.1 and Windows Server 2012 R2: KB4015550 and KB4015547.
Windows Server 2012	Critical	Remote Code Execution	Requires restart	Windows Server 2012: KB4015551 and KB4015548.
Windows RT 8.1	Critical	Remote Code Execution	Requires restart	Windows RT 8.1: KB4015550. Note: updates for Windows RT 8.1 are only available via Windows Update.
Windows 7 and Windows Server 2008 R2	Critical	Remote Code Execution	Requires restart	Windows 7 and Windows Server 2008 R2: KB4015549 and KB4015546.
Windows Vista and Windows Server 2008	Critical	Remote Code Execution	Requires restart	Updates for Windows Vista and Windows Server 2008 are not offered in a cumulative update or rollup. The following articles pertain to one of both operating systems: KB3211308, KB3217841, KB4014793, KB4015067, KB4015068, KB4015195, KB4015380, and KB4015383.
Internet Explorer	Critical	Remote Code Execution	Requires restart	Internet Explorer 9: KB4014661; Internet Explorer 10: KB4015551; Internet Explorer 11: KB4015217, KB4015219, KB4015221, KB4015550, and KB4015583.
Microsoft Silverlight	Important	Information Disclosure	May require a restart	Microsoft Silverlight: KB4017094. More information: https://www.microsoft.com/silverlight

Product Family	Maximum Severity	Maximum Impact	Restart Required?	Associated KB Articles and/or Support Webpages
.NET Framework	Critical	Remote Code Execution	May require a restart	There are 12 KB articles in this release covering the various versions of .NET Framework - too many to list here. Find links to these articles in the Security Update Guide.
Microsoft Office, Office Services, Office Web Apps, and other Office-related software	Critical	Remote Code Execution	May require a restart	There are 20 KB articles for Office components in this release - too many to list here. Find links to these articles in the Security Update Guide or visit the Office Tech Center landing page for Office Downloads and Updates.
Adobe Flash Player	Critical	Remote Code Execution	Requires restart	Information from Microsoft regarding security updates for Adobe Flash Player: KB4018483.
Visual Studio for Mac	Important	Information Disclosure	May require a restart	Resource webpage for Visual Studio for Mac: https://www.visualstudio.com/vs/visual-studio-mac/

Overview of vulnerabilities addressed in this release

Below is a summary showing the number of vulnerabilities addressed in this release, broken down by product/component and by impact.

Vulnerability Details (1)	RCE	EOP	ID	SFB	DOS	SPF	Publicly Disclosed	Known Exploit	Max CVSS
Windows 10 RTM	5	5	5	0	8	0	0	0	8.1
Windows 10 1511	5	5	5	0	8	0	0	0	8.1
Windows 10 1607 & Server 2016	5	4	5	1	9	0	0	0	8.1
Windows 10 1703	5	4	5	0	7	0	0	0	8.1
Windows 8.1 & Server 2012 R2	4	4	7	1	8	0	0	0	8.1
Windows Server 2012	4	3	6	0	6	0	0	0	8.1
Windows 7 & Server 2008 R2	3	3	4	0	5	0	0	0	8.1

Windows Vista & Server 2008	4	2	4	0	1	0	0	0	8.1
Internet Explorer	2	1	0	0	0	0	1	1	7.5
Microsoft Edge	3	0	1	1	0	0	1	0	4.3
Microsoft Silverlight	0	0	1	0	0	0	0	0	NA (2)
.NET Framework	1	0	0	0	0	0	0	0	NA (2)
Microsoft Office	3	1	1	1	0	1	1	2	NA (2)
Visual Studio for Mac	0	0	1	0	0	0	0	0	NA (2)
RCE = Remote Code Execution | EOP = Elevation of Privilege | ID = Information Disclosure SFB = Security Feature Bypass | DOS = Denial of Service | SPF = Spoofing									

(1) Vulnerabilities that overlap components may be represented more than once in the table.
(2) At the time of release, CVE scores were only available for Windows, Internet Explorer and Microsoft Edge.

Details on some of the vulnerabilities addressed in this release

Below are summaries for *some* of the security vulnerabilities in this release. These specific vulnerabilities were selected from the larger set of vulnerabilities in the release for one or more of the following reasons: 1) We received inquiries regarding the vulnerability; 2) the vulnerability may have received attention in the trade press; or 3) the vulnerability is potentially more impactful than others in the release. Because we do not provide summaries for every vulnerability in the release, you should review the content in the Security Update Guide for information not provided in these summaries.

CVE-2017-0166	**LDAP Elevation of Privilege Vulnerability**
Executive Summary	An elevation of privilege vulnerability exists when LDAP request buffer lengths are improperly calculated. An attacker who successfully exploited this vulnerability could run processes in an elevated context. The update addresses the vulnerability by correcting how LDAP request buffer lengths are calculated
Attack Vectors	In a remote attack scenario, an attacker could exploit this vulnerability by running a specially crafted application to send malicious traffic to a Domain Controller.
Mitigating Factors	Microsoft has not identified any mitigating factors for this vulnerability.
Workarounds	Microsoft has not identified any workarounds for this vulnerability.

Affected Software	All supported releases of Windows.
Impact	Elevation of Privilege
Severity	Important
Publicly Disclosed?	No
Known Exploits?	No
Exploitability Assessment Latest:	2 - Exploitation Less Likely
Exploitability Assessment Legacy:	2 - Exploitation Less Likely
More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0166

CVE-2017-0189	**Win32k Elevation of Privilege Vulnerability**
Executive Summary	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The update addresses this vulnerability by correcting how the Windows kernel-mode driver handles objects in memory
Attack Vectors	To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.
Mitigating Factors	Microsoft has not identified any mitigating factors for this vulnerability.
Workarounds	Microsoft has not identified any workarounds for this vulnerability.
Affected Software	All supported versions of Windows 10.
Impact	Elevation of Privilege
Severity	Important
Publicly Disclosed?	No
Known Exploits?	No
Exploitability Assessment Latest:	1 - Exploitation More Likely

Exploitability Assessment Legacy:	1 - Exploitation More Likely
More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0189

CVE-2017-0163	**Hyper-V Remote Code Execution Vulnerability**
Executive Summary	A remote code execution vulnerability exists when Windows Hyper-V Network Switch on a host server fails to properly validate input from an authenticated user on a guest operating system. An attacker who successfully exploited the vulnerability could execute arbitrary code on the host operating system. The security update addresses the vulnerability by correcting how Windows Hyper-V Network Switch validates guest operating system network traffic.
Attack Vectors	To exploit the vulnerability, an attacker could run a specially crafted application on a guest operating system that could cause the Hyper-V host operating system to execute arbitrary code.
Mitigating Factors	Customers who have not enabled the Hyper-V role are not affected.
Workarounds	Microsoft has not identified any workarounds for this vulnerability.
Affected Software	Windows 10, Windows 8.1, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016.
Impact	Remote Code Execution
Severity	Critical
Publicly Disclosed?	No
Known Exploits?	No
Exploitability Assessment Latest:	2 - Exploitation Less Likely
Exploitability Assessment Legacy:	2 - Exploitation Less Likely
More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0163

CVE-2017-0155	Windows Graphics Elevation of Privilege Vulnerability
Executive Summary	An elevation of privilege vulnerability exists in Windows when the Microsoft Graphics Component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The update addresses this vulnerability by correcting how the Microsoft Graphics Component handles objects in memory.
Attack Vectors	To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.
Mitigating Factors	Microsoft has not identified any mitigating factors for this vulnerability.
Workarounds	Microsoft has not identified any workarounds for this vulnerability.
Affected Software	Windows 7, Windows Server 2008, Windows Server 2008 R2, and Windows Vista.
Impact	Elevation of Privilege
Severity	Important
Publicly Disclosed?	No
Known Exploits?	No
Exploitability Assessment Latest:	1 - Exploitation More Likely
Exploitability Assessment Legacy:	1 - Exploitation More Likely
More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0155

CVE-2017-0202	Internet Explorer Memory Corruption Vulnerability
Executive Summary	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, the attacker could take control of an

	affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The update addresses the vulnerability by modifying how Internet Explorer handles objects in memory.
Attack Vectors	An attacker could host a specially crafted website designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. The attacker could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding specially crafted content that could exploit the vulnerability.
Mitigating Factors	An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by an enticement in an email or instant message, or by getting them to open an attachment sent through email. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. Accounts configured with fewer permissions would be at reduced risk.
Workarounds	Microsoft has not identified any workarounds for this vulnerability.
Affected Software	All supported versions of Internet Explorer.
Impact	Remote Code Execution
Severity	Critical
Publicly Disclosed?	No
Known Exploits?	No
Exploitability Assessment Latest:	1 - Exploitation More Likely
Exploitability Assessment Legacy:	1 - Exploitation More Likely
More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0202

CVE-2017-0201	**Scripting Engine Memory Corruption Vulnerability**
Executive Summary	A remote code execution vulnerability exists in the way that the JScript and VBScript engines render when handling objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with

	administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The update addresses the vulnerability by modifying how the JScript and VBScript scripting engines handle objects in memory.
Attack Vectors	In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.
Mitigating Factors	An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by an enticement in an email or instant message, or by getting them to open an attachment sent through email. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. Configuring accounts with fewer permissions would reduce risk.
Workarounds	Microsoft has not identified any workarounds for this vulnerability.
Affected Software	Internet Explorer 10 and Internet Explorer 9 on affected Windows clients and servers.
Impact	Remote Code Execution
Severity	Critical
Publicly Disclosed?	No
Known Exploits?	No
Exploitability Assessment Latest:	4 - Not affected
Exploitability Assessment Legacy:	1 - Exploitation More Likely
More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0201

CVE-2017-0210	**Internet Explorer Elevation of Privilege Vulnerability**
Executive Summary	An elevation of privilege vulnerability exists when Internet Explorer does not properly enforce cross-domain policies, which could allow an attacker to access information from one domain and inject it into another domain. An attacker who successfully exploited this vulnerability could elevate privileges in affected versions of Internet Explorer. The update addresses the vulnerability by helping to ensure that cross-domain policies are properly enforced in Internet Explorer.
Attack Vectors	The vulnerability by itself does not allow arbitrary code to be run. However, the vulnerability could be used in conjunction with another vulnerability (for example, a remote code execution vulnerability) that could take advantage of the elevated privileges when running arbitrary code. For example, an attacker could exploit another vulnerability to run arbitrary code through Internet Explorer, but due to the context in which processes are launched by Internet Explorer, the code might be restricted to run at a low integrity level (very limited permissions). However, an attacker could, in turn, exploit this vulnerability to cause the arbitrary code to run at a medium integrity level (permissions of the current user).
Mitigating Factors	An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action. For example, an attacker could trick users into clicking a link that takes them to the attacker's site.
Workarounds	Microsoft has not identified any workarounds for this vulnerability.
Affected Software	Internet Explorer 11 and Internet Explorer 10 on affected Windows clients and servers
Impact	Elevation on Privilege
Severity	Important
Publicly Disclosed?	Yes
Known Exploits?	Yes
Exploitability Assessment Latest:	0 - Exploitation Detected
Exploitability Assessment Legacy:	0 - Exploitation Detected
More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0210

CVE-2017-0200	Microsoft Edge Memory Corruption Vulnerability
Executive Summary	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that enables an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how Microsoft Edge handles objects in memory.
Attack Vectors	An attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge, and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements by adding specially crafted content that could exploit the vulnerability.
Mitigating Factors	An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by way of enticement in an email or Instant Messenger message, or by getting them to open an attachment sent through email. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. Configuring accounts with fewer permissions would reduce risk.
Workarounds	Microsoft has not identified any workarounds for this vulnerability.
Affected Software	Microsoft Edge
Impact	Remote Code Execution
Severity	Critical
Publicly Disclosed?	No
Known Exploits?	No
Exploitability Assessment Latest:	1 - Exploitation More Likely
Exploitability Assessment Legacy:	4 - Not affected
More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0200

CVE-2017-0093	Scripting Engine Memory Corruption Vulnerability
Executive Summary	A remote code execution vulnerability exists in the way that the Scripting Engine renders when handling objects in memory in Microsoft browsers. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. The security update addresses the vulnerability by modifying how the Scripting Engine handles objects in memory.
Attack Vectors	In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer or Microsoft Edge and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the scripting rendering engine. The attacker could also take advantage of compromised websites, and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerabilities.
Mitigating Factors	An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by an enticement in an email or instant message, or by getting them to open an attachment sent through email. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. Configuring accounts with fewer permissions would reduce risk.
Workarounds	Microsoft has not identified any workarounds for this vulnerability.
Affected Software	Microsoft Edge
Impact	Remote Code Execution
Severity	Critical
Publicly Disclosed?	No
Known Exploits?	No
Exploitability Assessment Latest:	1 - Exploitation More Likely
Exploitability Assessment Legacy:	4 - Not affected
More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0093

CVE-2017-0199	**Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows API**
Executive Summary	A remote code execution vulnerability exists in the way that Microsoft Office and WordPad parse specially crafted files. An attacker who successfully exploited this vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The update addresses the vulnerability by correcting the way that Microsoft Office and WordPad parses specially crafted files, and by enabling API functionality in Windows that Microsoft Office and WordPad will leverage to resolve the identified issue.
Attack Vectors	Exploitation of this vulnerability requires that a user open or preview a specially crafted file with an affected version of Microsoft Office or WordPad. In an email attack scenario, an attacker could exploit the vulnerability by sending a specially crafted file to the user and then convincing the user to open the file.
Mitigating Factors	An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to open or preview a specially crafted file with an affected version of Microsoft Office or WordPad.
Workarounds	Microsoft has not identified any workarounds for this vulnerability.
Affected Software	Microsoft Office 2007, Office 2010, Office 2013, Office 2016, Windows 7, Windows Vista, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012.
Impact	Critical
Severity	Remote Code Execution
Publicly Disclosed?	Yes
Known Exploits?	Yes
Exploitability Assessment Latest:	0 - Exploitation Detected
Exploitability Assessment Legacy:	0 - Exploitation Detected
More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199

CVE-2017-0195	Microsoft Office XSS Elevation of Privilege Vulnerability
Executive Summary	An elevation of privilege vulnerability exists when an Office Web Apps server does not properly sanitize a specially crafted request. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected Office Web Apps server. The attacker who successfully exploited this vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the victim, such as change permissions, delete content, steal sensitive information (such as browser cookies), and inject malicious content in the browser of the victim. The security update addresses the vulnerability by helping to ensure that Office Web Apps Server properly sanitizes web requests.
Attack Vectors	For the vulnerability to be exploited, a user must click a specially crafted URL that takes the user to a targeted Office Web App site. In an email attack scenario, an attacker could exploit the vulnerability by sending an email message containing the specially crafted URL to the user of the targeted Office Web App site and convincing the user to click the specially crafted URL. In a web-based attack scenario, an attacker would have to host a website that contains a specially crafted URL to the targeted SharePoint Web App site that is used to attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability.
Mitigating Factors	An attacker would have no way to force users to visit a specially crafted website. Instead, an attacker would have to convince them to visit the website, typically by getting them to click a link in an instant messenger or email message that takes them to the attacker's website, and then convince them to click the specially crafted URL. The attacker who successfully exploited this vulnerability could perform cross-site scripting attacks on affected systems and run scripts in the security context of the current user. Configuring user accounts to be more restricted would reduce risk for this vulnerability.
Workarounds	Microsoft has not identified any workarounds for this vulnerability.
Affected Software	Excel Services on SharePoint 2010 and SharePoint 2013, Excel Web App 2010, Office Web Apps 2010 and 2013, and Office Online Server.

Impact	Elevation of Privilege
Severity	Important
Publicly Disclosed?	No
Known Exploits?	No
Exploitability Assessment Latest:	2 - Exploitation Less Likely
Exploitability Assessment Legacy:	2 - Exploitation Less Likely
More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0195

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel (+971) 4 230 0003
Fax (+971) 4 230 0100
Email info[at]aeCERT.ae

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae