Advanced Notification of Microsoft Security Update Release – March 2017

Security Advisory AE-Advisory 17-14

Criticality Critical

Advisory Released On 15 March 2017

Purpose

To provide an overview of the latest security updates released by Microsoft on March 14, 2017.

Summary

aeCERT has received the latest Microsoft Security Update Release for March 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?	Servicing Notes
Windows 10 and Windows Server 2016	Critical	Remote Code Execution	Requires restart	Updates for Windows 10 and Windows Server 2016 will be cumulative, and will include both security fixes and non-security updates. For more information, see the TechNet resource Update Windows 10 In the Enterprise.
Windows 8.1 and Windows Server 2012 R2	Critical	Remote Code Execution	Requires restart	Updates for Windows 8.1 and Windows Server 2012 R2 will be offered via a single monthly rollup that addresses both security and reliability issues in a single update. A separate security-only rollup containing only security fixes for the month will also be available for download on the Microsoft Update Catalog. For more details, see Further simplifying servicing models for Windows 7 and Windows 8.1.
Windows Server 2012	Critical	Remote Code Execution	Requires restart	Updates for Windows Server 2012 will be offered via a single monthly rollup that addresses both security and reliability issues in a single update. A separate security-only rollup containing only security fixes for the month will also be available for download on the Microsoft Update Catalog. For more details, see Further simplifying servicing models for Windows 7 and Windows 8.1.
Windows RT 8.1	Critical	Remote Code Execution	Requires restart	Updates for Windows RT 8.1 and Microsoft Office RT software are only available via Windows Update.
Windows 7 and Windows Server 2008 R2	Critical	Remote Code Execution	Requires restart	Updates for Windows 7 and Windows Server 2008 R2 will be offered via a single monthly rollup that addresses both security and reliability issues in a single update. A separate security-only rollup containing only security fixes for the month will also be available for download on the Microsoft Update Catalog. For more details, see

Product Family	Maximum Severity	Maximum Impact	Restart Required?	Servicing Notes
				Further simplifying servicing models for Windows 7 and Windows 8.1.
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. Individual updates will be offered via Microsoft Update, Windows Update, and the Microsoft Update Catalog.
Microsoft Office, Office Services, Office Web Apps, and other Office-related software	Critical	Remote Code Execution	May require a restart	Updates for Office are offered through Microsoft Update and can also be downloaded separately. For information on updates for Microsoft Office, visit the Office Tech Center landing page for Office Downloads and Updates.
Internet Explorer	Critical	Remote Code Execution	Requires restart	The Security Only update for Windows 7, Windows Server 2008 R2, Windows Server 2012, Windows 8.1, and Windows Server 2012 R2 will not include security updates for Internet Explorer. These updates for IE will be offered as a separate package. For more details, see the blog post Simplified servicing for Windows 7 and Windows 8.1: the latest improvements.
Microsoft Silverlight	Critical	Remote Code Execution	May require a restart	Updates for Silverlight will be offered via Microsoft Update. For more information, please visit https://www.microsoft.com/silverlight
Microsoft Exchange Server	Important	Elevation of Privilege	May require a restart	Updates for Exchange will be offered via Microsoft Update and the Microsoft Download Center. Stay informed about Exchange via the Exchange Team Blog.
Adobe Flash Player	Critical	Remote Code Execution	Requires restart	Updates for Adobe Flash Player will be offered to the following operating systems: Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows RT 8.1, Windows 10, and Windows Server 2016. Further details regarding updates for Adobe Flash Player can be found in Adobe Security Bulletin APSB17-07.

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)	Remote Code Execution	Elevation of Privilege	Information Disclosure	Security Feature Bypass	Denial of Service	Spoofing	Publicly Disclosed	Known Exploit	Max CVSS
Windows 10 RTM	11	13	13	1	7	-	5	2	8.8
Windows 10 1511	10	15	12	1	6	-	5	2	8.8
Windows 10 1607 and Windows Server 2016	10	15	12	1	6	-	5	2	8.8
Windows 8.1 & Server 2012 R2	10	12	13	-	5	-	5	2	8.8
Windows Server 2012	10	12	11	1	4	-	4	2	8.8
Windows 7 & Server 2008 R2	18	10	31	-	3	-	4	2	8.8
Windows Vista & Server 2008	10	10	30	-	3	-	3	2	8.8
Internet Explorer	5	-	4	-	-	2	5	1	7.5
Microsoft Edge	21	-	5	3	-	3	5	-	4.3
Microsoft Silverlight	1	-	-	-	-	-	-	-	NA (2)
Microsoft Exchange	-	1	-	-	-	-	-	-	NA (2)
Microsoft Office	9	1	4	0	1	0	2	-	NA (2)

(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 were selected from the larger set for two reasons: 1) Microsoft has received inquiries regarding the vulnerabilities, or 2) the vulnerability is potentially more impactful than others in the release. Because Microsoft does 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-2017-0014	**Windows Graphics Component Remote Code Execution Vulnerability**
Executive Summary	A remote code execution vulnerability exists due to the way the Windows Graphics Component handles objects in the memory. An attacker who successfully exploited this vulnerability could take control of the 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 correcting how the Windows Graphics Component handles objects in the memory.
Attack Vectors	In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit this vulnerability and then convince a user to view the website. In a file-sharing attack scenario, an attacker could provide a specially crafted document file designed to exploit this vulnerability and then convince a user to open the document 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 take action, typically by getting them to click a link in an email or instant message that takes users to the attacker's website or by opening an attachment sent through email. 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.
Workarounds	Microsoft has not identified any workarounds for this vulnerability.
Affected Software	Windows 7, Windows 8.1, Windows RT 8.1, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows 10 , Windows Server 2016, Office 2010
Impact	Remote Code Execution
Severity	Critical

Publicly Disclosed?	Yes
Known Exploits?	No
Exploitability Assessment Latest:	2 - Exploitation Less Likely
Exploitability Assessment Legacy:	1 - Exploitation More Likely
More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0014

CVE-2017-0016	**SMBv2/SMBv3 Null Dereference Denial of Service Vulnerability**
Executive Summary	A denial of service vulnerability exists in implementations of the Microsoft Server Message Block 2.0 and 3.0 (SMBv2/SMBv3) client. The vulnerability is due to improper handling of certain requests sent by a malicious SMB server to the client. An attacker who successfully exploited this vulnerability could cause the affected system to stop responding until it is manually restarted. The security update addresses the vulnerability by correcting how the Microsoft SMBv2/SMBv3 Client handles specially crafted requests.
Attack Vectors	To exploit the vulnerability, an attacker could use various methods such as redirectors, injected HTML header links, etc., which could cause the SMB client to connect to a malicious SMB server.
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 8.1, Windows RT 8.1, Windows Server 2012 R2, Windows 10 , and Windows Server 2016.
Impact	Denial of Service
Severity	Important
Publicly Disclosed?	Yes
Known Exploits?	No
Exploitability Index Latest:	1 - Exploitation More Likely
Exploitability Index Legacy:	1 - Exploitation More Likely
More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0016

CVE-2017-0031	Microsoft Office Memory Corruption Vulnerability
Executive Summary	A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the 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 correcting how Office handles objects in memory.
Attack Vectors	Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) that contains a specially crafted file designed to exploit the vulnerability. Note that the Preview Pane is not an attack vector for this vulnerability.
Mitigating Factors	An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. 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.
Workarounds	Microsoft has not identified any workarounds for this vulnerability.
Affected Software	View the affected products for this vulnerability at the link below.
Impact	Remote Code Execution
Severity	Important
Publicly Disclosed?	No
Known Exploits?	No
Exploitability Index Latest:	4 – Not Affected
Exploitability Index Legacy:	1 - Exploitation More Likely

More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0031

CVE-2017-0035	**Scripting Engine Memory Corruption Vulnerability**
Executive Summary	A remote code execution vulnerability exists in the way affected Microsoft scripting engines render 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. 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 security update addresses the vulnerability by modifying how affected Microsoft scripting engines handle objects in memory.
Attack Vectors	In a web-based attack scenario, an attacker could host a specially crafted website designed to exploit the vulnerability through a Microsoft browser 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 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 getting them to click a link in an email or instant message that takes users to the attacker's website or by opening an attachment sent through email. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. Accounts configured to have fewer user rights on the system would be at lower risk than accounts configured with administrative user rights.
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 Index Latest:	1 - Exploitation More Likely
Exploitability Index Legacy:	4 – Not Affected
More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0035

CVE-2017-0037	**Microsoft Browser Memory Corruption Vulnerability**
Executive Summary	A remote code execution vulnerability exists when affected Microsoft browsers improperly access 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. In order to effect full code execution, an adversary would also need to combine this vulnerability with other exploits. An attacker who successfully combined multiple vulnerabilities to create an exploit chain 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 update addresses the vulnerability by modifying how Microsoft browsers handle objects in memory
Attack Vectors	An attacker could host a specially crafted website that is designed to exploit the vulnerability through affected Microsoft browsers, 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 getting them to click a link in an email or instant message that takes users to the attacker's website or by opening an attachment sent through email. An attacker who successfully exploited the vulnerability could gain the same user rights as the logged on account. Accounts configured to have fewer rights on the system would be at lower risk than accounts configured with administrative rights.

Workarounds	Microsoft has not identified any workarounds for this vulnerability.
Affected Software	Internet Explorer 10, Internet Explorer 11, and Microsoft Edge on affected Windows clients and servers.
Impact	Remote Code Execution
Severity	Critical
Publicly Disclosed?	Yes
Known Exploits?	No
Exploitability Index Latest:	1 - Exploitation More Likely
Exploitability Index Legacy:	1 - Exploitation More Likely
More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0037

CVE-2017-0038	**Windows Graphics Component Information Disclosure Vulnerability**
Executive Summary	Information disclosure vulnerability exist when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerabilities could obtain information to further compromise the user's system. The update addresses the vulnerability by correcting how the Windows GDI component handle objects in memory.
Attack Vectors	There are multiple ways an attacker could exploit the vulnerabilities, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage.
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 getting them to click a link in an email or instant message that takes users to the attacker's website, or by opening an attachment sent through email.
Workarounds	Microsoft has not identified any workarounds for this vulnerability.
Affected Software	Windows Vista, Windows 7, Windows 8.1, Windows RT 8.1, Windows Server 2008, Windows Server 2008 R2, Windows Server

	2012, Windows Server 2012 R2, Windows 10, and Windows Server 2016.
Impact	Information Disclosure
Severity	Important
Publicly Disclosed?	Yes
Known Exploits?	No
Exploitability Index Latest:	2 - Exploitation Less Likely
Exploitability Index Legacy:	2 - Exploitation Less Likely
More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0038

CVE-2017-0055	**Microsoft IIS Server XSS Elevation of Privilege Vulnerability**
Executive Summary	An elevation of privilege vulnerability exists when Microsoft IIS Server fails to properly sanitize a specially crafted request. An 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 behalf of the victim, and inject malicious content in the victim's browser. The security update addresses the vulnerability by correcting how Microsoft IIS Server sanitizes web requests.
Attack Vectors	For this vulnerability to be exploited, a user must click a specially crafted URL. In an email attack scenario, an attacker could exploit the vulnerability by sending an email message containing the specially crafted URL to the user and by convincing the user to click on the specially crafted URL. In a web-based attack scenario, an attacker would have to host a website that contains a specially crafted URL. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit this 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 getting them to click a link in an email or instant message that takes users to the

	attacker's website or by opening an attachment sent through email.
Workarounds	Microsoft has not identified any workarounds for this vulnerability.
Affected Software	Windows Vista, Windows 7, Windows 8.1, Windows RT 8.1, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows 10, and Windows Server 2016.
Impact	Elevation of Privilege
Severity	Important
Publicly Disclosed?	No
Known Exploits?	No
Exploitability Index Latest:	2 - Exploitation Less Likely
Exploitability Index Legacy:	2 - Exploitation Less Likely
More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0055

CVE-2017-0075	**Hyper-V Remote Code Execution Vulnerability**
Executive Summary	A remote code execution vulnerability exists when Windows Hyper-V 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 Hyper-V validates guest operating system user input.
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 Vista, Windows 7, Windows 8.1, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows 10, and Windows Server 2016.
Impact	Remote Code Execution

Severity	Critical
Publicly Disclosed?	No
Known Exploits?	No
Exploitability Index Latest:	2 - Exploitation Less Likely
Exploitability Index Legacy:	2 - Exploitation Less Likely
More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0075

CVE-2017-0084	**Uniscribe Remote Code Execution Vulnerability**
Executive Summary	A remote code execution vulnerability exists due to the way Windows Uniscribe handles objects in memory. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.
Attack Vectors	In a web-based attack scenario, an attacker could host a specially crafted website designed to exploit this vulnerability and then convince a user to view the website. In a file-sharing attack scenario, an attacker could provide a specially crafted document file designed to exploit this vulnerability and then convince a user to open the document 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 take action, typically by getting them to click a link in an email or instant message that takes users to the attacker's website, or by opening an attachment sent through email. 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.
Workarounds	Microsoft has not identified any workarounds for this vulnerability.
Affected Software	Windows Vista, Windows 7, Windows 8.1, Windows RT 8.1, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows 10, and Windows Server 2016.
Impact	Remote Code Execution

Severity	Critical
Publicly Disclosed?	No
Known Exploits?	No
Exploitability Index Latest	3 - Exploitation Unlikely
Exploitability Index Legacy	3 - Exploitation Unlikely
More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0084

CVE-2017-0107	**Microsoft SharePoint XSS Vulnerability**
Executive Summary	An elevation of privilege vulnerability exists when SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.
Attack Vectors	An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the 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 and delete content, and inject malicious content in the browser of the victim.
Mitigating Factors	A successful attack using this vulnerability requires that the attacker must first gain access (be able to log on) to the system. For this reason, it is most likely that this vulnerability would be used in combination with other vulnerabilities in a blended attack.
Workarounds	Microsoft has not identified any workarounds for this vulnerability.
Affected Software	Microsoft SharePoint Foundation 2013
Impact	Elevation of Privilege
Severity	Important
Publicly Disclosed?	No
Known Exploits?	No

Exploitability Index Latest:	4 – Not affected
Exploitability Index Legacy:	2 - Exploitation Less Likely
More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0107

CVE-2017-0108	**Graphics Component Remote Code Execution Vulnerability**
Executive Summary	A remote code execution vulnerability exists due to the way the Windows Graphics Component handles objects in the memory. An attacker who successfully exploited this vulnerability could take control of the 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 correcting how the Windows Graphics Component handles objects in the memory.
Attack Vectors	There are multiple ways an attacker could exploit this vulnerability. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit this vulnerability and then convince a user to view the website. In a file-sharing attack scenario, an attacker could provide a specially crafted document file designed to exploit this vulnerability and then convince a user to open the document 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 take action, typically by getting them to click a link in an email or instant message that takes users to the attacker's website, or by opening an attachment sent through email. 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.
Workarounds	Microsoft has not identified any workarounds for this vulnerability.
Affected Software	Windows Vista, Windows 7, Windows Server 2008, Windows Server 2008 R2, Lync 2010, Lync 2013, Skype for Business 2016, Office 2007, Office 2010, Word Viewer, and Silverlight 5.
Impact	Remote Code Execution

Severity	Critical
Publicly Disclosed?	No
Known Exploits?	No
Exploitability Index Latest:	3 - Exploitation Unlikely
Exploitability Index Legacy:	2 - Exploitation Less Likely
More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0108

CVE-2017-0110	**Microsoft Exchange Elevation of Privilege Vulnerability**
Executive Summary	An elevation of privilege vulnerability exists in the way that Microsoft Exchange Outlook Web Access (OWA) fails to properly handle web requests. An attacker who successfully exploited this vulnerability could perform script/content injection attacks and attempt to trick the user into disclosing sensitive information. The security update addresses the vulnerability by correcting how Microsoft Exchange validates web requests.
Attack Vectors	An attacker could exploit the vulnerability by sending a specially crafted email containing a malicious link to a user. Alternatively, an attacker could use a chat client to attempt to trick a user into clicking on their malicious link.
Mitigating Factors	An attacker would have no way to force users to click an unsafe link in an email or instant message.
Workarounds	Microsoft has not identified any workarounds for this vulnerability.
Affected Software	Exchange Server 2013 Cumulative Update 14, Exchange Server 2013 SP1, and Exchange Server 2016 Cumulative Update 3.
Impact	Elevation of Privilege
Severity	Important
Publicly Disclosed?	No
Known Exploits?	No
Exploitability Index Latest:	3 - Exploitation Unlikely
Exploitability Index Legacy:	3 - Exploitation Unlikely

More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0110

CVE-2017-0143	**Windows SMB Remote Code Execution Vulnerability**
Executive Summary	A remote code execution vulnerability exists in how the Microsoft Server Message Block 1.0 (SMBv1) service handles certain requests. An attacker who successfully exploited this vulnerability could gain code execution on the target server. This security update addresses the vulnerability by correcting how SMBv1 handles these specially crafted requests.
Attack Vectors	To exploit the vulnerability, an attacker would need to negotiate a connection to SMBv1 as part of the attack.
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 Vista, Windows 7, Windows 8.1, Windows RT 8.1, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows 10, and Windows Server 2016.
Impact	Remote Code Execution
Severity	Critical
Publicly Disclosed?	No
Known Exploits?	No
Exploitability Index Latest:	1 - Exploitation More Likely
Exploitability Index Legacy:	1 - Exploitation More Likely
More Details	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0143

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