Advanced Notification of Microsoft Office/WordPad Remote Code Execution Vulnerability

Security Advisory AE-Advisory 17-20

Criticality Critical 

Advisory Released On 13 April 2017

CVE Reference ID

CVE-2017-0199

Impact

Arbitrary code execution

Affected Software

Primary Products		
Microsoft, Inc.	Office	2007 (SP3) | 2010 (SP2, 32-bit editions, 64-bit editions) | 2016 (Base, 32-bit editions, 64-bit editions)

Associated Products		
Microsoft, Inc.	Windows 7	for 32-bit systems (SP1) | for x64-based systems (SP1)
	Windows Server 2008	Datacenter Edition (SP2) | Datacenter Edition, 64-bit (SP2) | Itanium-Based Systems Edition (SP2) | Enterprise Edition (SP2) | Enterprise Edition, 64-bit (SP2) | Essential Business Server Standard (SP2) | Essential Business Server Premium (SP2) | Essential Business Server Premium, 64-bit (SP2) | Standard Edition (SP2) | Standard Edition, 64-bit (SP2) | Web Server (SP2) | Web Server, 64-bit (SP2)
	Windows Server 2012	Original Release (Base)
	Windows Vista	Home Basic (SP2) | Home Premium (SP2) | Business (SP2) | Enterprise (SP2) | Ultimate (SP2) | Home Basic x64 Edition (SP2) | Home Premium x64 Edition (SP2) | Business x64 Edition (SP2) | Enterprise x64 Edition (SP2) | Ultimate x64 Edition (SP2)

Solution

Refer to the “Solution” section below

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found out about a new critical vulnerability in Microsoft Office that could allow an unauthenticated remote attacker to run arbitrary commands on a targeted system. Further information is explained in the Threat Details section below.

Threat Details

Vulnerability Details:

The vulnerability consists of the affected software improperly parsing crafted email messages. An attacker is able to exploit the vulnerability by sending a specially crafted email to a victim. This email message is designed specifically to submit malicious input to the affected software and use misleading language/instructions to persuade a user to open the email message. If successful, the attacker is able to execute arbitrary code and completely compromise the target system thus gaining full control of the machine.

As an example, the exploitation of this vulnerability requires that the user opens or previews a specially crafted file with an affected version of Microsoft Office or WordPad. So, the attacker sends the email message in a persuasive form making the victim eager to open the message. Once, the message is opened, the email message gets parsed in an abnormal way and the attacker is able to execute arbitrary commands and take control of the machine as mentioned above.

Microsoft's notes:

Microsoft has confirmed that the vulnerability exists in a security bulletin and released software updates to fix it. Please refer to the Solution section below for further information on how to avoid being a victim of this critical vulnerability.

Solution

- Administrators are advised to apply the appropriate updates
- Administrators are advised to only allow trusted users to have network access
- We recommend that users do not open email messages from suspicious or unrecognized sources. If a user is not able to verify the links/attachments included in an email message, then they are advised to not open them
- Administrators are advised to use an unprivileged account when browsing the Internet
- Administrators are advised to monitor critical systems continuously
- You can obtain updates by using the links in the Microsoft Security Bulletin. You can also update using Microsoft Update service on every Windows operating system
- This attack cannot bypass the Office Protected View feature, aeCERT recommends that this feature is enabled on Microsoft Office products, for more information, visit the below URL: https://support.office.com/en-us/article/What-is-Protected-View-d6f09ac7-e6b9-4495-8e43-2bbcdbcb6653

Best Practices

These are the best practices that are recommended to be followed:

- Ensure all IT systems (OSs, applications, websites, AV…etc.) are updated.
- Ensure that your security systems are current, can inspect deeply and can detect and prevent phases of attack plan.
- Ensure relevant third party and support vendors are aware and accessible encase of an infection.
- Probe any anomalous network and system behavior and examine it. Make sure your system is not infected.

- Remind users to be particularly careful and watch out for phishing and spear-phishing emails. Be cautious when opening e-mail attachments and check if the file extension corresponds to the file name.
- Only response to trusted emails and only visit trusted websites as a precaution.
- Plan or review your incident response procedures with all necessary parties (not only IT groups). Explore how the planned response against such infection.
- Monitor any suspicious and anonymous IP sources or destinations in your network. Keep track of these IPs and make sure they are not reported as suspicious or malicious addresses.

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