Advanced Notification of Wormable Vulnerability in Remote Desktop Services

Security Advisory	ADV-19-20	**Criticality**	High	
Advisory Released On	15 May 2019			

Impact

A vulnerability on Microsoft operating systems that include Remote Desktop Services could be exploited by attackers to widely spread malware.

Solution

Adhere the advices written under the recommendations section.

Affected Platforms:

- Windows 2003
- Windows XP
- Windows 7
- Windows Server 2008
- Windows Server 2008 R2

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT would like to inform you that Microsoft has released a security update addressing a critical vulnerability found in Remote Desktop Services. This vulnerability allows malware to spread in a similar fashion to the widely spread WannaCry malware as it is pre-authentication and doesn't require any interaction from the user's side.

Details

The vulnerability is located in the Remote Desktop Services which was previously known as Terminal Services. An unauthenticated attacker can exploit this vulnerability by remotely connecting to the target system and sending specifically created requests.

The Remote Desktop Protocol (RDP) is not vulnerable as this vulnerability is found pre-authentication and does not require any input or interaction from the user's side. This makes the vulnerability "wormable" which means that malware could widely spread between computers that have the same vulnerability. This type of attack was previously seen back in 2017 when the WannaCry malware was widely spreading.

Microsoft has reported that this vulnerability has not been exploited at the time of writing this report and it does not affect Windows 8.1 or 10 and Windows Server 2012 and above. It does however affect Windows 7 and Windows Server 2008 and 2008 R2 as well as previous unsupported operating systems such as XP and 2003.

Recommendations

In order to circumvent the exploit, we highly recommend the following:

- Frequently download the latest patches released by Microsoft.
- Enable Network Level Authentication (NLA) to authenticate Remote Desktop Services requests.
- We highly advise upgrading your operating system if it is unsupported by Microsoft.

Disclaimer

Accessing third-party links in this advisory will direct you to an external website. Please note that aeCERT bears no responsibility for third-party website traffic. aeCERT will have no liability to the entities for the content or use of the content available through the hyperlinks that are referenced

References

Prevent a worm by updating Remote Desktop Services

CVE-2019-0708

Microsoft patches Windows XP and Server 2003 to prevent Wormable flaw

Contact Us

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

Tel (+971) 4 777 4003
Fax (+971) 4 777 4100
Email info[at]aeCERT.ae
Instagram @TheUAETRA
Twitter @TheUAETRA

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