TLP: WHITE

# Advisory Alert

**Alert No: AAA20200318** **Date: 18-Mar-20 12:00 PM**

**Classification** **The Alert : Public Circulation Permitted**

## Security Updates for 18th March 2020

| | | |
|---|---|---|
| **Overview** | **High** | **Microsoft** • **Patch released for the vulnerability in SMBv3**<br>**VMware** • **Privilege escalation vulnerabilities** |
| **Description / Impact** | **Microsoft** | • SMBv3.11 contains a buffer overflow vulnerability (CVE-2020-0796) when compression is enabled (default configuration). Windows 10 and Windows Servers use SMBv3.11 and the service runs as SYSTEM. Attacker can send a specially crafted packet targeting a SMBv3 server to exploit the vulnerability which will result in remote code execution, with SYSTEM privileges. The security update addresses the vulnerability by correcting how the SMBv3 protocol handles these specially crafted requests.<br>• Officially Acknowledged by the Vendor: **Yes** |
| | **VMware** | • The vulnerability will lead to remote code execution on the host computer from the guest computer or it will allow attackers to create a denial of service condition of the vmnetdhcp service running on the host machine.<br>• Affected Products:<br>• **VMware Workstation Pro / Player**<br>• **VMware Fusion Pro / Fusion**<br>• **VMware Horizon Client for Windows**<br>• **VMware Remote Console for Windows**<br>• Officially Acknowledged by the Vendor: **Yes** |
| **Additional Information** | **Visit the links below and follow the instructions given by respective vendors according to your internal policies/ procedures.**<br>**Microsoft** | • https://support.microsoft.com/en-us/help/4551762/windows-10-update-kb4551762<br>• https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796 |
| | **VMware** | • https://www.vmware.com/security/advisories/VMSA-2020-0004.html |
| **Disclaimer** | The information provided herein is on "as is" basis, without warranty of any kind. | |