Advisory Alert

Alert No: AAA200312 **Date: 12-MAR-20 09.45 AM**

Classification **The Alert : Public Circulation Permitted**

Multiple Vulnerabilities

Overview	**High**	**Microsoft** **Microsoft** **Intel** **Linux**	■ **Multiple Vulnerabilities** ■ **Arbitrary code execution** ■ **Load Value Injection vulnerability** ■ **Arbitrary code execution**

Description / Impact

Microsoft

- Microsoft has released its March 2020 Security Update which addresses multiple vulnerabilities across several of its products, which an attacker could use to gain control of an affected system.
- Affected Products:
  - **Microsoft Windows**
  - **Microsoft Edge (EdgeHTML-based)**
  - **Microsoft Edge (Chromium-based)**
  - **Internet Explorer**
  - **Microsoft Exchange Server**
  - **Microsoft Office and Microsoft Office Services and Web Apps**
  - **Azure DevOps**
  - **Windows Defender**
  - **Azure**
  - **Microsoft Dynamics**
- Officially Acknowledged by the Vendor: **Yes**

Microsoft

- A new wormable vulnerability has been discovered in Microsoft SMBv3 (Server Message Block 3.0) which exists in the handling of compression, Successful exploitation could allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable system.
- Affected Products:
  - **Windows 10 Version 1903 for 32-bit Systems**
  - **Windows 10 Version 1903 for ARM64-based Systems**
  - **Windows 10 Version 1903 for x64-based Systems**
  - **Windows 10 Version 1909 for 32-bit Systems**
  - **Windows 10 Version 1909 for ARM64-based Systems**
  - **Windows 10 Version 1909 for x64-based Systems**
  - **Windows Server, version 1903 (Server Core installation)**
  - **Windows Server, version 1909 (Server Core installation)**
- Officially Acknowledged by the Vendor: **Yes**

Intel

- A new security flaw in Intel processors has been identified and tracked as **CVE-2020-0551.** Successful exploitation could allow a less privileged attacker to steal sensitive information and take significant control over a targeted system.
- Affected Products:
  - **Intel CPUs**
- Officially Acknowledged by the Vendor: **Yes**

Linux

- A Vulnerability has been discovered in the Extensible Authentication Protocol (EAP) packet processing in the Point-to-Point Protocol Daemon (pppd) software that comes installed on Linux based operating systems. An unauthenticated remote attacker could use this vulnerability to cause a stack buffer overflow, which may allow arbitrary code execution on the target system.
- Affected Products:
  - **pppd in ppp 2.4.2 through 2.4.8**
- 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.

Microsoft	https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Mar
Microsoft	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/adv200005
Intel	https://software.intel.com/security-software-guidance/software-guidance/load-value-injection
Linux	https://www.debian.org/security/2020/dsa-4632 https://access.redhat.com/errata/RHSA-2020:0631

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.