TLP: WHITE

Advisory Alert

Alert No: AAA20200513 **Date: 13-May-20 12:30 PM**

Classification **The Alert : Public Circulation Permitted**

Security Updates for 13th May 2020

Overview	**High** **Microsoft** • **Multiple Vulnerabilities** **Cisco** • **File Policy Bypass Vulnerability**
Description / Impact	**Microsoft** . Microsoft has released its May 2020 Security Update which address 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** • **Windows Defender** • **Microsoft Dynamics** • **.NET Framework** • **.NET Core** Officially Acknowledged by the Vendor: **Yes** **Cisco** . Cisco Multiple products are affected by File Policy Bypass Vulnerability that could allow an attacker to compromise and remotely perform arbitrary actions on an affected device. . Affected Products: • **1000 Series Integrated Services Routers** • **3000 Series Industrial Security Appliances** • **4000 Series Integrated Services Routers** • **Cloud Services Router 1000V Series** • **Firepower Threat Defense (FTD) Software** • **Integrated Services Virtual Router** . 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-May **Cisco** • https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort_filepolbypass-m4X5DgOP
Disclaimer	The information provided herein is on "as is" basis, without warranty of any kind.