Vulnerability in various Products for May 11 -20, 2020, as informed by CERT-In for necessary actions

Deatiled Vulnerability Note may be seen from CERT-In Website

https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2020-XXXX, substituting XXXX with the number in second column

Kindly confirm action taken by your organisation in the enclosed compliance sheet.

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
10	CIVN-2020-0152	Microsoft Internet Explorer Windows 10 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1709 for 32-bit Systems Windows 10 Version 1709 for 64-based Systems Windows 10 Version 1709 for	It could be exploited by a remote attacker to execute arbitrary code on a targeted system.	HIGH	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1035

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1058

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1060

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1062

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1064

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1092

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1093 |

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		ARM64-based Systems Windows 10 Version 1803 for 32-bit Systems Windows 10 Version 1803 for ARM64-based Systems Windows 10 Version 1803 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1903 for 32-bit Systems Windows 10 Version 1903 for ARM64-based Systems			

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		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 7 for 32-bit Systems Service Pack 1 Windows 7 for x64-based Systems Service Pack 1 Windows 8.1 for 32-bit systems Windows 8.1 for x64-based systems Windows RT 8.1 Windows Server 2008 for 32-bit Systems Service			

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		Pack 2 Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019			
11	CIVN-2020-0153	Acrobat DC and Acrobat Reader DC(Continuous Track) version 2020.006.20042 and prior for Windows and MacOS Acrobat 2017 and Acrobat Reader 2017 version 2017.011.30166 and prior for Windows and	It could be exploited by an attacker to execute arbitrary code, obtain sensitive information, bypass security features or cause denial-of-service (DoS) conditions on a targeted system.	HIGH	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		MacOS Acrobat 2015 and Acrobat Reader 2015 version 2015.006.30518 and prior for Windows and MacOS			
17	CIVN-2020-0161	Microsoft Edge (Edge HTML-based). Microsoft Internet Explorer 10. Microsoft Chakra Core. Windows Server 2019.	It could be exploited by a remote attacker to bypass security restrictions and execute arbitrary code on the targeted system.	HIGH	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1037
34	CIVN-2020-0178	Windows 10 for x64-based Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1709 for x64-based	It could allow an attacker to bypass security restrictions, may cause denial of service condition (DoS), access sensitive information, gain elevated privileges	HIGH	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0909 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0963 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1010 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1021

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		Systems Windows 10 Version 1803 for x64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1903 for x64-based Systems Windows 10 Version 1909 for x64-based Systems Windows 7 for x64-based Systems SP1 Windows 8.1 for x64-based systems Windows Server 2008 for x64-based Systems SP2 & Server Core installation Windows Server 2008 R2 for x64-based Systems	and execute arbitrary code on the targeted system.		https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1028 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1048 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1051 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1054 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1055 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1061 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1067 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1068 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1070 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1071 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1072 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1075 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		SP1 & Server Core installation Windows Server 2012 & Server Core installation Windows Server 2012 R2 & Server Core installation Windows Server 2016 & Server Core installation Windows Server 2019 & Server Core installation Windows Server, version 1803 (Server Core Installation) Windows Server, version 1903 (Server Core installation) Windows Server, version 1909 (Server Core installation)			2020-1076 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1077 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1078 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1079 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1081 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1082 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1084 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1086 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1087 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1088 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1090 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1109 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
					2020-1110
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1111
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1112
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1113
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1114
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1116
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1117
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1118
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1121
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1123
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1124
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1125
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
					2020-1126
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1131
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1132
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1134
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1135
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1136
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1137
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1138
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1139
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1140
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1141
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1142
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
					2020-1143
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1144
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1145
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1149
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1151
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1153
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1154
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1155
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1156
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1157
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1158
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1164
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
					2020-1165
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1166
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1174
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1175
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1176
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1179
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1184
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1185
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1186
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1187
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1188
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1189
					https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
					2020-1190 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1191

Vulnerability in various Products for May 20-31, 2020, as informed by CERT-In for necessary actions

Deatiled Vulnerability Note may be seen from CERT-In Website

https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2020-XXXX, substituting XXXX with the number in second column

Kindly confirm action taken by your organisation in the enclosed compliance sheet.

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
8	CIVN-2020-186	Microsoft Edge (Chromium-based) versions prior to 83.0.478.37	It could allow a remote attacker to gain elevated privileges on a targeted system.	MEDIUM	Update to version 83.0.478.37 as mentioned at https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1195
15	CIVN-2020-193	Google Chrome versions prior to 83.0.4103.61	It could be exploited by a remote attacker to execute arbitrary code on the targeted system.	HIGH	Upgrade to Google chrome version 83.0.4103.61 as mentioned in: https://chromereleases.googleblog.com/2020/05/stable-channel-update-for-desktop_19.html
20	CIAD-2020-0031	All Bluetooth devices supporting BR/EDR Core Configurations version 5.2 and prior	A vulnerability has been reported in Bluetooth protocol, which could be exploited by an adjacent attacker to	MEDIUM	It is highly recommended that the end users apply the latest update. Bluetooth host and controller suppliers should refer to the Bluetooth SIG for guidance on updating their products. https://www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/bluetooth-security/bias-vulnerability/

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
			perform a spoofing attack(BIAS) impersonating the address of a previously paired remote device. An attacker with physical access to the Bluetooth connection could perform a spoofing attack impersonating the address of a previously paired remote device. This attack may result in the attacking device completing the authentication procedure successfully despite not		

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
			possessing the link key.		