Vulnerability in various Products for June 21-30, 2020, as informed by CERT-In for necessary actions

Detailed 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
2	CIVN-2020-0223	Google Chrome	It could allow a remote attacker to execute arbitrary code, conduct spoofing attack, bypass security restrictions and access sensitive information on the targeted system.	HIGH	https://chromereleases.googleblog.com/2020/06/stable-channel-update-for-desktop.html
5	CIVN-2020-0226	Microsoft ChakraCore Internet Explorer 11 Microsoft Edge (EdgeHTML-based)	Memory Corruption vulnerability has been reported in Microsoft browsers which could allow remote attacker to execute arbitrary code on the targeted system.	HIGH	https://portal.msrc.microsoft.com/en-US/security-guidance

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
8	CIVN-2020-0229	1. Windows 10 Version 1709 for 32-bit Systems and x64-based Systems 2. Windows 10 Version 1709 for ARM64-based Systems 3. Windows 10 Version 1803 for 32-bit Systems and x64-based Systems 4. Windows 10 Version 1803 for ARM64-based Systems 5. Windows 10 Version 1809 for 32-bit Systems and x64-based Systems 6. Windows 10 Version 1809 for ARM64-based Systems 7. Windows 10 Version 1903 for 32-bit Systems and x64-based Systems 8. Windows 10 Version 1903 for ARM64-based Systems 9. Windows 10 Version 1909 for 32-bit Systems and x64-based Systems 10. Windows 10 Version 1909 for ARM64-based Systems 11. Windows 10 Version 2004 for 32-bit Systems and x64-based Systems 12. Windows 10 Version 2004 for ARM64-based Systems 13. Windows Server	A remote code execution vulnerability has been reported in Windows shell which could allow an attacker to bypass security restrictions, access sensitive information and execute arbitrary code to gain elevated privileges on the targeted system.	HIGH	https://portal.msrc.microsoft.com/en-US/security-guidance

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		2019(Server Core Installation also affected) 14. Windows Server, version 1803 (Server Core Installation also affected) 15. Windows Server, version 1903 (Server Core installation) 16. Windows Server, version 1909 (Server Core installation) 17. Windows Server, version 2004 (Server Core installation)			
11	CIVN-2020-0232	Cisco Webex Meetings Desktop App	Multiple Code Execution vulnerability have been reported in the software update feature of Cisco Webex Meetings Desktop App which could allow an unauthenticated, remote attacker to execute arbitrary code and programs on an affected system.	HIGH	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-client-mac-X7vp65BL https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-client-url-fcmpdfVY

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
12	CIVN-2020-0233	Cisco Webex Meetings	Unauthorized Access vulnerability have been reported in Cisco Webex Meetings and Cisco Webex Meetings Server which could allow an unauthenticated, remote attacker to gain unauthorized access to a vulnerable Webex site.	HIGH	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-token-zPvEjKN
14	CIVN-2020-0235	Google Chrome versions prior to 83.0.4103.106	It could allow a remote attacker to execute arbitrary code or bypass security restrictions on the targeted system.	HIGH	Upgrade to Google Chrome 83.0.4103.106 as mentioned in: https://chromereleases.googleblog.com/2020/06/stable-channel-update-for-desktop_15.html
15	CIVN-2020-0236	Windows 7 for 32-bit and x64-based SP 1 ·Windows 8.1 for 32-bit and x64-based systems ·Windows RT 8.1 ·Windows 10 for 32-bit and x64-based Systems	Remote code execution vulnerability has been reported in Microsoft Windows which could allow a	HIGH	https://portal.msrc.microsoft.com/en-us/security-guidance

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		·Windows 10 Version 1607 for 32-bit and x64-based Systems ·Windows 10 Version 1709 for 32-bit, x64-based and ARM64-based Systems ·Windows 10 Version 1803 for 32-bit, x64-based and ARM64-based Systems ·Windows 10 Version 1809 for 32-bit, x64-based and ARM64-based Systems ·Windows 10 Version 1903 for 32-bit, x64-based and ARM64-based Systems ·Windows 10 Version 1909 for 32-bit, x64-based and ARM64-based Systems ·Windows 10 Version 2004 for 32-bit, x64-based and ARM64-based Systems ·Windows Server 2008 for 32-bit SP 2 and 32-bit SP 2 (Server Core installation) ·Windows Server 2008 for Itanium-Based SP 2 ·Windows Server 2008 R2 for Itanium-Based SP 1 ·Windows Server 2008 R2 for x64-based SP 1 and x64-based SP 1 (Server Core installation) ·Windows Server 2012 and	remote attacker to trigger a remote code execution on target system.		

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		2012 (Server Core installation) ·Windows Server 2012 R2 and 2012 R2 (Server Core installation) ·Windows Server 2016 and 2016 (Server Core installation) ·Windows Server 2019 and 2019 (Server Core installation) ·Windows Server, version 1803, 1903, 1909 and 2004 (Server Core Installation)			
16	CIVN-2020-0237	Internet Explorer 11 for 1. Windows 10 Version 2004 for x64-based Systems and ARM64-based Systems 2. Windows 10 Version 1803 for 32-bit Systems, x64-based Systems and ARM64-based Systems 3. Windows 10 Version 1809 for 32-bit Systems, x64-based Systems and ARM64-based Systems 4. Windows 10 Version 1909 for 32-bit Systems, x64-based Systems and ARM64-based Systems	Multiple remote code execution vulnerabilities has been reported in Microsoft VBScript which could allow a remote attacker to execute arbitrary code on the targeted system.	HIGH	https://portal.msrc.microsoft.com/en-us/security-guidance

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		5. Windows 10 Version 1709 for 32-bit Systems, x64-based Systems and ARM64-based Systems 6. Windows 10 Version 1903 for 32-bit Systems, x64-based Systems and ARM64-based Systems 7. Windows 10 Version 1607 for 32-bit Systems and for x64-based Systems 8. Windows 10 for 32-bit Systems and x64-based Systems 9. Windows 10 Version 2004 for 32-bit Systems 10. Windows 7 for 32-bit Systems Service Pack 1 and x64-based Systems Service Pack 1 11. Windows 8.1 for 32-bit systems and x64-based systems 12. Windows Server 2008 R2 for x64-based Systems Service Pack 1 13. Windows RT 8.1 14. Windows Server 2012 R2 15. Windows Server 2012 16. Windows Server 2016			

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		17. Windows Server 2019 18. Internet Explorer 9 for 19. Windows Server 2008 for 32-bit Systems Service Pack 2 20. Windows Server 2008 for x64-based Systems Service Pack 2			
22	CIVN-2020-0243	Cisco Webex Meetings Desktop App for Windows releases prior to 40.4.12 and 40.6.0.	Information Disclosure vulnerability have been reported in Cisco Webex Meetings Desktop App for Windows which could allow an authenticated, local attacker to gain access to sensitive information on an affected system.	HIGH	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-client-NBmqM9vt (At the time of publication, Cisco Webex Meetings Desktop App for Windows release 40.4.12 and releases 40.6.0 and later contained the fix for this vulnerability. For lockdown versions of Cisco Webex Meetings Desktop App for Windows, releases 39.5.26 and later contained the fix for this vulnerability) Upgrade to the latest version
26	CIVN-2020-0247	Google Chrome versions prior to 83.0.4103.116	Use-After-Free vulnerability has been reported in Google Chrome that could allow a remote attacker to execute arbitrary code on the	HIGH	Upgrade to Google Chrome 83.0.4103.116 https://chromereleases.googleblog.com/2020/06/stable-channel-update-for-desktop_22.html

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
			targeted system.		
35	CIAD-2020-0040	COVID 19-related Phishing Attack Campaign by Malicious Actors	The phishing campaign is expected to use malicious emails under the pretext of local authorities in charge of dispensing government-funded Covid-19 support initiatives. Such emails are designed to drive recipients towards fake websites where they are deceived into downloading malicious files or entering personal and financial information.		https://zeenews.india.com/india/north-koreas-lazarus-hackers-plan-phishing-attack-in-india-to-steal-covid-aid-2290701.html