Vulnerability in various Products for January 11-20, 2022, 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-2022-XXXX, substituting XXXX with the number in second column

Please update the below mentioned applications/window's version to latest version to avoid security risks. Kindly confirm action taken in your organization.

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
6	CIVN-2022-0024	Privilege Escalation Vulnerability in Microsoft Windows Active Directory Domain Services •Windows Server 2012 R2 (Server Core installation) •Windows Server 2012 R2 •Windows Server 2012 (Server Core installation) •Windows Server 2012 •Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) •Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) •Windows Server 2008 for x64-based Systems Service Pack 2 •Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) •Windows Server 2008 for 32-bit Systems Service Pack 2 •Windows RT 8.1 •Windows 8.1 for x64-based systems •Windows 8.1 for 32-bit systems •Windows 7 for x64-based Systems Service Pack 1 •Windows 7 for 32-bit Systems Service Pack 1 •Windows Server 2016 (Server Core installation) •Windows Server 2016 •Windows 10 Version 1607 for x64-based Systems	It has been reported that a vulnerability exists in Microsoft Windows Active Directory Domain Services which allow a remote authenticated attacker to escalate privileges on the vulnerable system.	HIGH	Apply appropriate patch as mentioned in Microsofts advisory: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21857

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Windows 10 Version 1607 for 32-bit Systems •Windows 10 for x64-based Systems •Windows 10 for 32-bit Systems •Windows 10 Version 21H2 for x64-based Systems •Windows 10 Version 21H2 for ARM64-based Systems •Windows 10 Version 21H2 for 32-bit Systems •Windows 11 for ARM64-based Systems •Windows 11 for x64-based Systems •Windows Server, version 20H2 (Server Core Installation) •Windows 10 Version 20H2 for ARM64-based Systems •Windows 10 Version 20H2 for 32-bit Systems •Windows 10 Version 20H2 for x64-based Systems •Windows Server 2022 (Server Core installation) •Windows Server 2022 •Windows 10 Version 21H1 for 32-bit Systems •Windows 10 Version 21H1 for ARM64-based Systems •Windows 10 Version 21H1 for x64-based Systems •Windows 10 Version 1909 for ARM64-based Systems •Windows 10 Version 1909 for x64-based Systems •Windows 10 Version 1909 for 32-bit Systems •Windows Server 2019 (Server Core installation) •Windows Server 2019 •Windows 10 Version 1809 for ARM64-based Systems •Windows 10 Version 1809 for x64-based Systems •Windows 10 Version 1809 for 32-bit Systems			
8	CIVN-2022-0026	Remote Code Execution Vulnerability in Windows IKE Extension •Windows Server 2016 (Server Core installation) •Windows Server 2016 •Windows 10 Version 1607 for x64-based Systems •Windows 10 Version 1607 for 32-bit Systems •Windows 10 for x64-based Systems •Windows 10 for 32-bit Systems	A remote code execution vulnerability has been reported in Windows Internet Key Exchange (IKE) Extension which could allow a remote attacker to execute arbitrary code on the targeted system.	HIGH	Apply appropriate patches as mentioned by vendor

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Windows 10 Version 21H2 for x64-based Systems •Windows 10 Version 21H2 for ARM64-based Systems •Windows 10 Version 21H2 for 32-bit Systems •Windows 11 for ARM64-based Systems •Windows 11 for x64-based Systems •Windows Server, version 20H2 (Server Core Installation) •Windows 10 Version 20H2 for ARM64-based Systems •Windows 10 Version 20H2 for 32-bit Systems •Windows 10 Version 20H2 for x64-based Systems •Windows Server 2022 (Server Core installation) •Windows Server 2022 •Windows 10 Version 21H1 for 32-bit Systems •Windows 10 Version 21H1 for ARM64-based Systems •Windows 10 Version 21H1 for x64-based Systems •Windows 10 Version 1909 for ARM64-based Systems •Windows 10 Version 1909 for x64-based Systems •Windows 10 Version 1909 for 32-bit Systems •Windows Server 2019 (Server Core installation) •Windows Server 2019 •Windows 10 Version 1809 for ARM64-based Systems •Windows 10 Version 1809 for x64-based Systems •Windows 10 Version 1809 for 32-bit Systems			https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21849
16	CIVN-2022-0034	Remote code execution vulnerability in Microsoft Windows •Microsoft Windows Server 2019 and 2019 (Server Core installation) •Microsoft Windows 10 Version 1809 for 32-bit, x64-based and ARM64-based Systems •Microsoft Windows 10 Version 1909 for 32-bit, x64-based and ARM64-based Systems •Microsoft Windows 10 Version 20H2 for 32-bit, x64-based and ARM64-based Systems •Microsoft Windows Server, version 20H2 (Server Core Installation) •Microsoft Windows 10 Version 21H1 for 32-bit, x64-based and	A vulnerability has been reported in Microsoft Windows which could allow a remote attacker to trigger a remote code execution on target system.	HIGH	Apply appropriate patches as mentioned in Microsoft Security Bulletin: https://msrc.mi-

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		ARM64-based Systems •Microsoft Windows 10 Version 21H2 for 32-bit, x64-based and ARM64-based Systems •Microsoft Windows 11 version for x64-based and ARM64-based Systems •Microsoft Windows Server 2022 and 2022 (Server Core installation)			crosoft.com/update-guide/vulnerability/CVE-2021-22947
18	CIVN-2022-0036	Privilege Escalation Vulnerability in Microsoft Windows Virtual Machine IDE Drive •Windows Server 2012 R2 (Server Core installation) •Windows Server 2012 R2 (Server Core installation) •Windows Server 2012 R2 •Windows Server 2012 R2 •Windows Server 2012 (Server Core installation) •Windows Server 2012 (Server Core installation) •Windows Server 2012 •Windows Server 2012 •Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) •Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) •Windows Server 2008 R2 for x64-based Systems Service Pack 1 •Windows Server 2008 R2 for x64-based Systems Service Pack 1 •Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) •Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) •Windows Server 2008 for x64-based Systems Service Pack 2 •Windows Server 2008 for x64-based Systems Service Pack 2 •Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) •Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	A Privilege Escalation Vulnerability has been reported in Microsoft Windows Virtual Machine IDE Drive which could allow a local authenticated attacker to execute arbitrary code on the targeted system.	HIGH	Apply appropriate patches as mentioned by vendor https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21833

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat De-scription	Vulnerability Rating	Vendor URL/ Action
		•Windows Server 2008 for 32-bit Systems Service Pack 2 •Windows Server 2008 for 32-bit Systems Service Pack 2 •Windows RT 8.1 •Windows 8.1 for x64-based systems •Windows 8.1 for x64-based systems •Windows 8.1 for 32-bit systems •Windows 8.1 for 32-bit systems •Windows 7 for x64-based Systems Service Pack 1 •Windows 7 for x64-based Systems Service Pack 1 •Windows 7 for 32-bit Systems Service Pack 1 •Windows 7 for 32-bit Systems Service Pack 1 •Windows Server 2016 (Server Core installation) •Windows Server 2016 •Windows 10 Version 1607 for x64-based Systems •Windows 10 Version 1607 for 32-bit Systems •Windows 10 for x64-based Systems •Windows 10 for 32-bit Systems •Windows 10 Version 21H2 for x64-based Systems •Windows 10 Version 21H2 for ARM64-based Systems •Windows 10 Version 21H2 for 32-bit Systems •Windows 11 for ARM64-based Systems •Windows 11 for x64-based Systems •Windows Server, version 20H2 (Server Core Installation) •Windows 10 Version 20H2 for ARM64-based Systems •Windows 10 Version 20H2 for 32-bit Systems •Windows 10 Version 20H2 for x64-based Systems •Windows Server 2022 (Server Core installation) •Windows Server 2022 •Windows 10 Version 21H1 for 32-bit Systems •Windows 10 Version 21H1 for ARM64-based Systems •Windows 10 Version 21H1 for x64-based Systems •Windows 10 Version 1909 for ARM64-based Systems			

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Windows 10 Version 1909 for x64-based Systems •Windows 10 Version 1909 for 32-bit Systems •Windows Server 2019 (Server Core installation) •Windows Server 2019 •Windows 10 Version 1809 for ARM64-based Systems •Windows 10 Version 1809 for x64-based Systems •Windows 10 Version 1809 for 32-bit Systems			
20	CIVN-2022-0038	Multiple Vulnerabilities in Mozilla Products •Mozilla Firefox versions prior to 96 •Mozilla Firefox ESR versions prior to 91.5 •Mozilla Firefox Thunderbird versions prior to 91.5	Multiple vulnerabilities have been reported in Mozilla products which could allow a remote attacker to bypass security restriction, execute arbitrary code and cause denial of service attack on the targeted system.	HIGH	Upgrade to Mozilla Firefox version Firefox 96, Firefox ESR 91.5 and Thunderbird 91.5
22	CIVN-2022-0040	Multiple Vulnerabilities in Google Chrome •Google Chrome versions prior to 97.0.4692.99	Multiple vulnerabilities have been reported in Google Chrome which could be exploited by a remote attacker to bypass security restrictions, execute arbitrary code or cause denial of service condition on the targeted system.	HIGH	Apply appropriate updates as mentioned https://chromereleases.google-blog.com/2022/01/stable-channel-update-for-desktop_19.html