Vulnerability in various Products for October 01-31, 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 act ion taken in your organisation.

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
15	CIVN-2022-0387	Arbitrary Code Execution Vulnerability in LibreOffice •LibreOffice versions prior to 7.3.6/7.4.1	A vulnerability has been reported in Libre office which could allow an attacker to execute arbitrary code on the targeted system.	MEDIUM	Successful exploitation of this vulnerability could allow an attacker to run arbitrary script execution without warning on the targeted system.
16	CIVN-2022-0388	Multiple Vulnerabilities in Google Chrome for Desktop •Google Chrome versions prior to 106.0.5249.119	Multiple Vulnerabilities have been reported in Google Chrome for Desktop which could be exploited by a remote attacker to bypass security restriction, execute arbitrary code or cause denial of service condition on the targeted system.	HIGH	Apply appropriate updates as mentioned by the vendor: https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_11.html
17	CIVN-2022-0389	Multiple Vulnerabilities in Adobe Acrobat and Reader •Acrobat DC and Acrobat Reader DC (Continuous) versions 22.002.20212 and earlier for Windows & MacOS.	Multiple vulnerabilities have been reported in Adobe Acrobat and Reader which could allow an attacker to obtain sensitive information, exe-	HIGH	Apply appropriate updates as mentioned in the Adobe Security Bulletin: https://helpx.adobe.com/

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Acrobat 2020 and Acrobat Reader 2020 (Classic 2020) versions 20.005.30381 and earlier for Windows & MacOS.	cute arbitrary code and denial of service on the targeted system.		security/products/acrobat/apsb22-46.html
20	CIVN-2022-0392	Privilege Elevation Vulnerability in Windows COM+ Event System Service •Windows Server 2022 (Server Core installation) •Windows Server 2022 •Windows Server 2019 (Server Core installation) •Windows Server 2019 •Windows Server 2016 (Server Core installation) •Windows Server 2016 •Windows Server 2012 R2 (Server Core installation) •Windows Server 2012 R2 •Windows Server 2012 (Server Core installation) •Windows Server 2012 •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 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 RT 8.1	A vulnerability has been reported in Windows COM+ Event System Service which could allow local authenticated attacker to gain elevated privileges and to execute arbitrary code on the targeted system.	HIGH	Apply appropriate upgrade as mention: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41033

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•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 11 for x64-based Systems •Windows 11 for ARM64-based Systems •Windows 11 Version 22H2 for x64-based Systems •Windows 11 Version 22H2 for ARM64-based 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 10 Version 21H1 for x64-based Systems •Windows 10 Version 21H1 for ARM64-based Systems •Windows 10 Version 21H1 for 32-bit Systems •Windows 10 Version 20H2 for x64-based Systems •Windows 10 Version 20H2 for ARM64-based Systems •Windows 10 Version 20H2 for 32-bit Systems •Windows 10 Version 1809 for x64-based Systems •Windows 10 Version 1809 for ARM64-based Systems •Windows 10 Version 1809 for 32-bit Systems			

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Windows 10 Version 1607 for x64-based Systems •Windows 10 Version 1607 for 32-bit Systems			
34	CIVN-2022-0406	Multiple Vulnerabilities in Mozilla Products •Mozilla Firefox ESR versions prior to 102.4 •Mozilla Firefox versions prior to 106	Multiple vulnerabilities have been reported in Mozilla products which could allow a remote attacker to bypass security restrictions, execute arbitrary code and cause denial of service attack on the targeted system.	HIGH	Upgrade to Mozilla Firefox ESR version 102.4 and Mozilla Firefox version 106 as mentioned by the vendor
40	CIVN-2022-0412	Multiple Vulnerabilities in Google Chrome •Google Chrome versions prior to 107.0.5304.62 for Mac. •Google Chrome versions prior to 107.0.5304.68 for linux. •Google Chrome versions prior to 107.0.5304.62/63 for Windows.	Multiple vulnerabilities have been reported in Google Chrome which could be exploited by an attacker to bypass security restriction, execute arbitrary code or cause denial of service condition on the targeted system.	HIGH	Apply appropriate updates as mentioned by Vendor: https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_25.html
44	CIAD-2022-0026	Password Management and Security •Cloud-based options can be more flexible to access from wherever you need, easier to set up and easier to maintain. However, it does require trusting the provider and ensure that the solution is hosted within India. •Locally hosted options require less trust in external parties, but requires ongoing maintenance. It may limit your ability to access from external locations such as staff working remotely. Cloud or locally hosted solutions may	Disclaimer	Be of at least 8 characters in length Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z) Have at least one numerical character (e.g. 0-9) Have at least one special character (e.g. ~!@#$%^&*()_-+=) Systems should be designed to accept and transmit passwords with proper safeguards such as	Contact Information

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		be chosen according to organization's need. •The password management solutions should have up-to-date encryption algorithms with multiple layers of encryption. •Strong encryption key practices are also important in the cases of cloud-based password management solutions. •Multi-factor authentication should be used for accessing the password database and resetting master password, especially if the password management solution is cloud-based. •Secure and safe provisions should be used for sharing Shared passwords with authorized people. •Logging information features should be used to see every time a user views or copies a password for traceability. •The password management solutions should have features to generate passwords or passphrases, which can be set to generate minimum or maximum length passwords.		Passwords should not be displayed while entered and also should not be saved in web browsers Passwords should not be stored in clear text or in automated login script Passwords must be secured with Multifactor authentication (MFA). Password hashes must be protected Use pass phrases for encryption An effective password management or password vault solution may be used within organisation, and made available for all staff. Utilise password management solutions or password vault solutions to set policies to auto-generate long & unique passwords and to periodically change passwords. Required Security features for Password management	