Vulnerability in various Products for July 11-20, 2021, 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-2021-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-2021-0166 | •Acrobat DC and Acrobat Reader DC (Continuous) versions 2021.005.20054 and prior for Windows & macOS •Acrobat DC and Acrobat Reader DC (Classic 2020) versions 2020.004.30005 and prior for Windows & macOS •Acrobat DC and Acrobat Reader DC (Classic 2017) versions 2017.011.30197and prior for Windows & macOS | Multiple vulnerabilities have been reported in Acrobat DC and Acrobat Reader DC which could allow an attacker to execute arbitrary code, gain escalated privileges, read and write arbitrary system files and cause denial of service condition on the targeted system. | High | https://helpx.adobe.com/security/products/acrobat/apsb21-51.html |
| 3 | CIVN-2021-0167 | •Mozilla Firefox versions prior to 90 •Mozilla Firefox ESR versions prior to 78.12 •Mozilla Thunderbird versions prior to 78.12 | Multiple vulnerabilities have been reported in Mozilla Products which could allow remote attacker to execute arbitrary code, escalate privileges, disclose potentially sensitive information, or cause denial of service conditions on the target system. | High | https://www.mozilla.org/en-US/security/advisories/mfsa2021-28/ https://www.mozilla.org/en-US/security/advisories/mfsa2021-29/ https://www.mozilla.org/en-US/security/advisories/mfsa2021-30/ |

| S No | CERT-in Vulnerability Note No | Product | Vulnerability Threat Description | Vulnerability Rating | Vendor URL/ Action |
|---|---|---|---|---|---|
| 5 | CIAD-2021-0024 | •Windows<br>•Microsoft Office<br>•Extended Security Updates (ESU)<br>•Developer Tools<br>•SQL Server<br>•Exchange Server<br>•Microsoft Dynamics<br>•System Center<br>•Apps | Multiple vulnerabilities have been reported in various Microsoft products, which could be exploited by an attacker to access sensitive information, bypass security restrictions, perform a denial of service (DoS) attack, escalating privileges, perform Spoofing attacks or executing arbitrary codes on the targeted system. | High | Apply appropriate security updates as mentioned in<br><br>https://msrc.microsoft.com/update-guide/en-us/releaseNote/2021-Jul |