#5 Dominion Voting Systems, the second-largest U.S. election machine vendor, which has given public presentations acknowledging their use of modems in their voting machines, was also discovered to be running remote-access software during the 2020 election:

In Georgia, 20-year election worker, Susan Voyles, testified that Dominion Voting Systems employees "operated remotely" on her ballot-marking devices and poll pads after the team experienced some technical problems with their machines.

In Wisconsin, the Office of Special Counsel (OSC), headed by former state Supreme Court Justice Michael Gableman, also found that Dominion and ES&S voting machines were online and connected to the internet.

In Michigan, attorney and Secretary of State candidate Matt Deperno, discovered a Telit LE910-SV1 modem chip embedded in the motherboard of an ES&S DS200 voting machine.

Through these modems, hackers could theoretically intercept results as they're transmitted on election night — or, worse, use the modem connections to reach back into voting machines or the election management systems to install malware, change software, or alter official results.

Therefore, not only are hackers able to penetrate elections through vulnerable USB cards and election management systems but also through the very voting machines themselves.