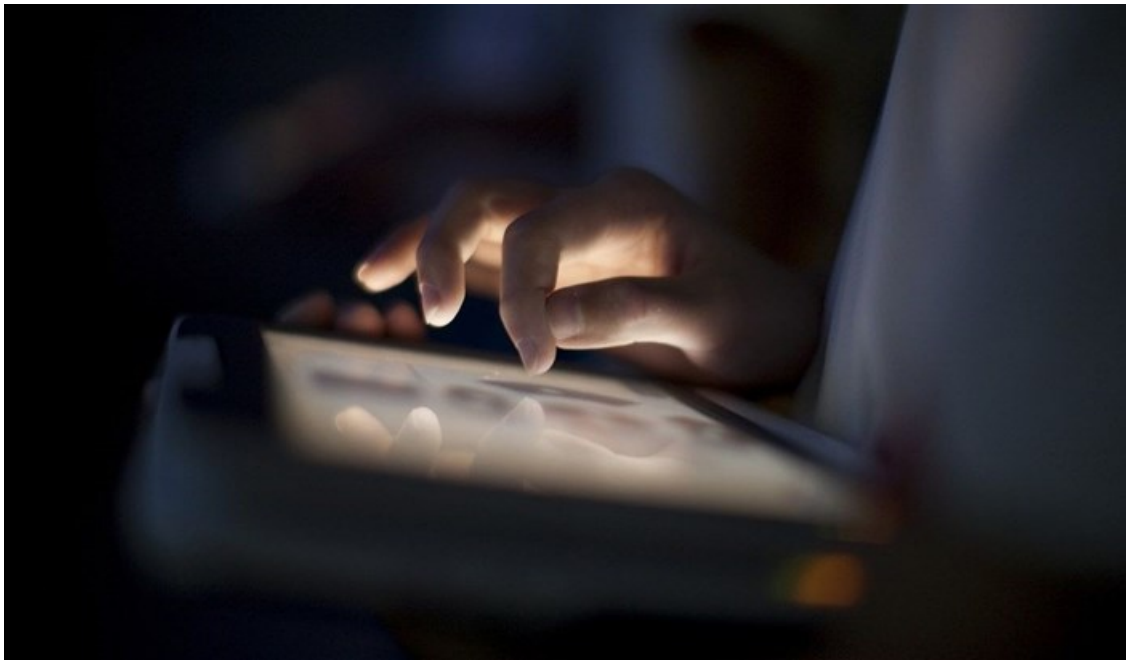
Connected electric car chargers could damage home networks

While modern electric vehicles are tested constantly for vulnerabilities, some of their essential accessories, such as the battery chargers, often remain neglected.

Kaspersky Lab experts have discovered that electric vehicle (EV) chargers supplied by a major vendor carry vulnerabilities that can be exploited by cyber attackers, and that the consequences of a successful attack could include damage to the home electricity network.

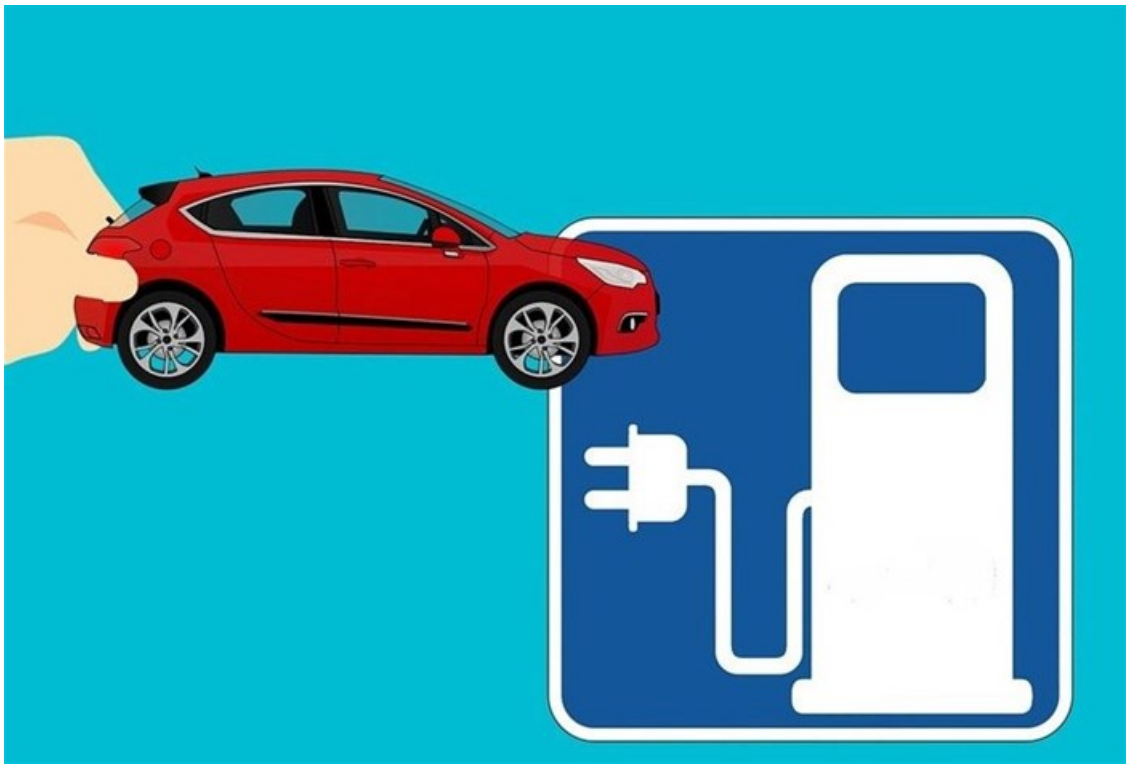


Electric vehicles are a hot topic as their development makes a vital contribution to environmental sustainability.

In some regions, public and private charging points are becoming commonplace. The growing popularity of electric vehicles led Kaspersky Lab experts to check widely available domestic chargers that include a remote access feature.

The researchers found that, if compromised, the connected charger could cause a power overload that would take down the network it was connected to, causing both financial impact and, in the worst-case scenario, damaging other devices connected to the network.

The researchers found a way to initiate commands on the charger and to either stop the charging processor or set it to the maximum current possible. While the first option would only prevent a person from using the car, the second one could potentially cause the wires to overheat on a device that is not protected by a trip fuse.



Source: pixabay.com

All an attacker needs to do to change the amount of electricity being consumed is obtain Wi-Fi access to the network the charger is connected to. Since the devices are made for domestic use, security for the wireless network is likely to be limited.

This means that attackers could gain access easily, for example by brute-forcing all possible password options, which is quite common: according to Kaspersky Lab statistics, 94% of attacks on IoT in 2018 came from Telnet and SSH password brute-forcing. Once inside the wireless network, the intruders can easily find the charger's IP-address. This, in turn, will allow them to exploit any vulnerabilities and disrupt operations.

All the vulnerabilities found were reported to the vendor and have now been patched.

> *"People often forget that in a targeted attack, cybercriminals always look for the least-obvious elements to compromise in order to remain unnoticed. This is why it is very important to look for vulnerabilities, not just into unresearched technical innovations, but also in their accessories – they are usually a coveted prize for threat actors. As we have shown, vendors should be extra careful with connected vehicle devices, and initiate bug-bounties or ask cybersecurity experts to check their devices. In this case, we were fortunate to have a positive response and a rapid patch of the devices, which helped to prevent potential attacks," said Dmitry Sklyar, a security researcher at Kaspersky Lab.*

Kaspersky Lab recommends taking the following security measures:

- Regularly update all your smart devices to the latest software versions. Updates may contain patches for critical vulnerabilities, which, if left unpatched, may give cybercriminals access to your house and private life.

- Don't use the default password for Wi-Fi routers and other devices, change it to strong ones and don't use the same password for several devices.

- We recommend isolating the smart home network from the network used by your or your family’s personal devices for basic internet searching. This is to ensure that if a device is compromised with generic malware through a phishing email, your smart home system won’t be affected.

For more, visit: https://www.bizcommunity.com