Siemens Patches CCTV Camera Hijacking Bug

Siemens said IP-based CCTV cameras bearing its brand are vulnerable to attacks that could allow them to be taken over by anyone with access to the devices over the Internet.

The company said a list of camera products contain a bug that could allow remote attackers to gain administrative credentials by sending specially crafted requests to the device's built-in web server.

Patch available

It said Vanderbilt Industries, which acquired the Siemens IP Cameras business last year, has made a patch available and urged users to apply it.

"Until patches can be applied, restricting access to the integrated web server with appropriate mechanisms is recommended," Siemens said in an advisory.

The company said in general it recommends the cameras be operated within trusted networks that are protected by perimeter security measures.

It also recommends enabling authentication on the device's web server, which isn't switched on by default.

The lack of security of Internet-connected devices, sometimes collectively called the "Internet of Things", has received more attention recently following a disruptive attack that made use, in part, of hacked gadgets to cut off access to a number of high-profile websites.

The October denial-of-service attack on DNS provider Dyn was carried out in part using traffic generated by a Mirai botnet, which drew on hacked IP cameras, set-top boxes and the like.

It resulted in limited access to sites such as Twitter, Amazon, Reddit and Netflix.

US and EU regulators have suggested taking action to improve IoT security, but several billion

insecure devices are already in use around the world.

Many of them use default administrative credentials that are publicly known, meaning they can be taken over without the need to exploit a software bug.

Do you know all about security in 2016? Try our quiz!