Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Security News of the Week

by Thomas Martin, Manchester Metropolitan University, Senior Lecturer

Tuesday 3rd August 2021

Warship positions faked including UK aircraft carrier

AIS (Automatic Identification System) is used by many large sea vessels to determine their position. However, it has been recently discovered that certain ships have had their positions spoofed, that AIS was telling them they were somewhere they were not. A UK carrier strike group was among the almost 100 impacted vessels. Researchers were able to determine the discrepancy by studying satellite imagery and AIS data, although they do not yet know how the system was corrupted nor who was responsible. Read more>

Home car charger owners urged to install updates

Anyone is possession of a home electric car charger is being advised to obtain and apply the latest security patches. Researchers at Pen Test Partners found several serious security issues with chargers by Wallbox and Project EV. By exploiting vulnerabilities, they were able to gain full control of the charger and so could charge any car for free, disable the charger permanently, or attack other chargers/servers. They were also able to obtain access to home wi-fi networks. Patches have been released for the software vulnerabilities, but the researchers also pointed out that the use of a Raspberry Pi by Wallbox has inherent weaknesses that cannot be patched in software. Read more>

Google Chrome to no longer show secure website indicators

Google Chrome is no longer going to show a padlock icon in the address bar to indicate the site is using HTTPS. Any site using HTTP will have a "Not secure" warning, and the use of HTTPS will be inferred by the warning's absence. Google have been encouraging the adoption of HTTPS for a while, by giving secure sites higher rankings in search results. The change will come into effect in Chrome 93. Read more>

Joint advisory on top cyber vulnerabilities

A list of the most commonly exploited vulnerabilities since 2020 has been released. The list was compiled jointly by the Australian Cyber Security Centre (ACSC), the UK's National Cyber Security Centre (NCSC), and the US Federal Bureau of Investigation (FBI). Products that are commonly attacked include those of Microsoft, Pulse, Accellion, VMware, and Fortinet, with attention being paid to systems involved in remote work, VPNs, or cloud technology. While many of the exploits were disclosed recently in 2020/2021, some go as far back as 2017. Administrators are encouraged to apply security fixes for all commonly exploited vulnerabilities. Read more>

European Union
European Regional Development Fund
Manchester Metropolitan University
MANCHESTER 1824 The University of Manchester
University of Salford MANCHESTER
Lancaster University