Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Security News of the Week

by Thomas Martin, Manchester Metropolitan University, Senior Lecturer

Tuesday 27th July 2021

Windows "HiveNightmare" bug could leak passwords – here's what to do!

Separate from the "PrintNightmare" problem, Microsoft have disclosed another security issue that could impact users. The "HiveNightmare" vulnerability could allow unprivileged user to read sensitive information from the system registry. The problem stems from incorrect access permissions assigned to the registry hive files. The hive files are locked for access by the OS only, but any copies taken in system restore points are not similarly restricted. Microsoft have released instructions on how to correctly block the hive files from unauthorised access. Read more>

Windows "PetitPotam" network attack – how to protect against it

A French researcher has released a proof-of-concept of a Windows exploit, furthering the security headaches at Microsoft. The attack is a new form of NTLM relay to bypass authentication. NTLM has been depreciated by Microsoft for a decade, but still persists because of legacy systems that still require it. Previous NTLM relay attacks used systems such as the Microsoft Print System Remote Protocol, but this new issue takes advantage of the Encrypting File System Remote Protocol. The main mitigation suggested is removing all use of NTLM, but Microsoft have also released some steps that can provide immediate mitigation for the problem (but with no guarantee that similar issues will not crop up later). Read more>

Ransomware key to unlock customer data from REvil attack

The IT firm Kaseya had been hit by a ransomware attack by the REvil group. However, a "trusted third party" has provided a decryption key. Kaseya can use that key to recover their files as well as the files of the hundreds of the customer organisations that were also impacted. It is not known who provided the key or why, but there is speculation that this could be a sign that REvil is winding down its operations.
Read more>

Signal fixes bug that sent random images to wrong contacts

The privacy-oriented messaging app has released a patch to fix an unusual and worrisome bug. Back in December 2020, users were reporting that multiple images were being sent when only one was intended. The problem was eventually identified as a database issue on the client, where an identifier was not set to AUTOINCREMENT and so repetitions were occurring. Signal faced difficulty in reproducing the issue as they did not initially collect user logs (for added privacy). They needed to add this capability before they could get the information needed to discover what was going wrong.
Read more>

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