Windows 10/11 vulnerability exposes admin passwords to local users

July 21 2021, by Bob Yirka

Credit: Pixabay/CC0 Public Domain

A Twitter user has found and made public a Windows 10/11 vulnerability that exposes admin passwords to local users who can then escalate their privileges up to admin, giving them total system access. As he notes on his posts, he found that Windows Security Account Manager

(SAM) data could be read by users with very limited privileges, giving them access to admin passwords. Microsoft apparently caught wind of the vulnerability and posted an Executive Summary of the issue on its Security Vulnerability page.

The news of a new vulnerability in the Windows operating system is not good for Microsoft, coming just weeks after warnings about the PrintNightmare vulnerability in Windows Print Spooler. Microsoft says this new vulnerability is a result of inadequate protection of access control lists on several system files, which include the SAM database. They further note that an unauthorized person could use the vulnerability to run custom code that takes advantage of higher system privileges and could add, change or delete user data. They conclude by noting that unauthorized users would need to have the ability to run code on such systems to be able to take advantage of the vulnerability.

Others on Twitter and elsewhere have noted the vulnerability exists only for systems running build 1809 of Windows 10 and some versions of Windows 11. They note also that in addition to allowing access to SAM data, the vulnerability also allows access to certain system and security files. For a nefarious person to take advantage of the vulnerability, the system must have a VSS shadow copy of the system drive. This copy may exist on user systems due to inadvertent actions they may have taken, such as installing a hard drive that holds more than 128GB and then conducting a Windows update. Adding an installer package file format called MSI will do so, as well. Users who want to know if their system has the vulnerability can run the system command vssadmin.

Microsoft notes that they will update customers as they learn more. No timeline for a patch has yet been announced.

More information: msrc.microsoft.com/update-guid … ility/CVE-2021-36934