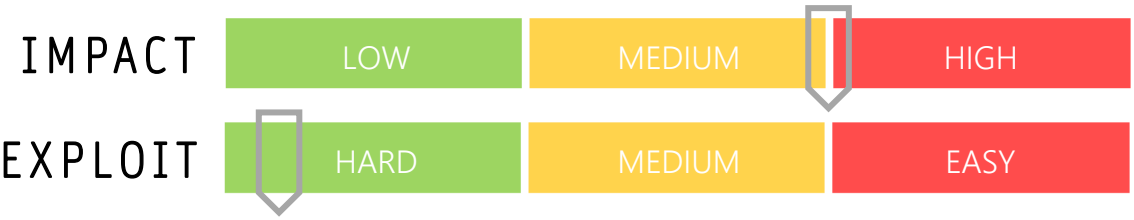
UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

# CYBER GUIDANCE ISSUE 00176

## SERIOUSSAM WORKAROUND ISSUED BY MICROSOFT

**DATE ISSUED:** 26th July 2021




## OVERVIEW

The zero-day dubbed SeriousSAM (also known as HiveNightmare) has no patch available, so Microsoft have issued a workaround for Windows 10 to prevent the local privilege escalation attacks on vulnerable systems. One researcher discovered that the not-yet-released Windows 11 is also at risk.

## BREAKDOWN

Systems vulnerable to the SeriousSAM exploit include all Windows Client and Server versions released since October 2018 (Windows 10 189 & Windows Server 2019). By exploiting incorrect file permissions, attackers may be able to steal a privileged account's NTLM password hash to gain elevated privilege using the "pass-the-hash" technique. From there, low privileged users will be able to access Registry database files. Attackers will not be able to directly access databases, as this will trigger access violations, they are however, able to access the Volume Shadow Copy Service (VSS). It is important to note that disabling or removing shadow copies may hinder restore operations in the event disaster recovery plans are required to be activated. CVE-2021-36934

## REMEDIATION STEPS

- See resources for full instructions on how to implement the workaround issued by Microsoft.

## REFERENCES & RESOURCES

| | |
|---|---|
| Bleeping Computer | https://www.bleepingcomputer.com/news/microsoft/microsoft-shares-workaround-for-windows-10-serioussam-vulnerability/ |
| Microsoft | https://support.microsoft.com/en-us/topic/kb5005357-delete-volume-shadow-copies-1ceaa637-aaa3-4b58-a48b-baf72a2fa9e7 |
| | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934 |
| Threatpost | https://threatpost.com/win-10-serioussam/168034/ |
| GitHub PoC | https://github.com/GossiTheDog/HiveNightmare |