HC3: Sector Alert

July 30, 2021 TLP: White Report: 202107301400

HiveNightmare/SeriousSAM Potential HPH Impact

Executive Summary

Microsoft identified a vulnerability which can allow an attacker to gain administrative privileges or execute code of their choice on certain Windows systems, including many Windows client and server versions released since October 2018. HC3 recommends that healthcare organizations ensure they review the list of recommended mitigations in this document and apply them appropriately for all impacted systems in their infrastructure.

Report

A researcher recently disclosed a trivially exploitable vulnerability (CVE-2021-36934) in various deployments of Windows 10 and 11 that can allow a local, non-administrative user to obtain administrative access and/or execute arbitrary code on a system. Successful exploitation of this vulnerability allows an attacker to access registry files stored in folders such as SYSTEM, SECURITY, SAM, DEFAULT, and SOFTWARE. The Security Account Manager (SAM) folder in particular contains hashed passwords for all users on a system, which threat actors can exploit and then use to assume their identity. Windows 10 and Windows 11 registry files associated with SAM and all other registry databases, are accessible to members of the "Users" group who typically only have low privileges. Historically, members of the "Users" group are numerous and relatively easy to compromise, making this issue more egregious. Another security researcher published proof-of-concept for this exploit. It was initially believed to only impact Windows 10 and 11, but Microsoft announced that it also impacts many Windows client and server versions released since October 2018, beginning with Windows 10 release 1809 and Windows Server 2019. This vulnerability has a base CVSS score of 7.8, was initially publicly released on July 20, 2021 and was last updated (as of this report) on July 27, 2021.

Mitigations

There is currently no patch available for this vulnerability, as of July 30, 2021. Microsoft maintains a dedicated knowledgebase article which provides technical details and will include information on a patch, when it becomes available. Microsoft recommends the following:

- Restrict access to the contents of %windir%\system32\config
  - Command Prompt (Run as administrator):
    icacls %windir%\system32\config*.* /inheritance:e
  - Windows PowerShell (Run as administrator):
    icacls $env:windir\system32\config*.* /inheritance:e
- Delete Volume Shadow Copy Service (VSS) shadow copies
  - Identify whether Shadow volumes exist with either Command Prompt or PowerShell (Run as administrator):
    - vssadmin list shadows
  - Delete any System Restore points and Shadow volumes that existed prior to restricting access to the contents of %windir%\system32\config
- Delete Volume Shadow Copy Service (VSS) shadow copies
  - Identify whether Shadow volumes exist with either Command Prompt or PowerShell (Run as administrator):
    - vssadmin list shadows

Delete any System Restore points and Shadow volumes that existed prior to restricting access to the contents of

%windir%\system32\config

References

NIST: CVE-2021-36934 Detail
https://nvd.nist.gov/vuln/detail/CVE-2021-36934

Microsoft Windows Elevation of Privilege Vulnerability (CVE-2021-36934)
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934

New Windows 10 vulnerability allows anyone to get admin privileges
https://www.bleepingcomputer.com/news/microsoft/new-windows-10-vulnerability-allows-anyone-to-get-admin-privileges/

SeriousSAM bug impacts all Windows 10 versions released in the past 2.5 years
https://therecord.media/serioussam-bug-impacts-all-windows-10-versions-released-in-the-past-2-5-years/

Microsoft SAM File Readability CVE-2021-36934: What You Need to Know
https://www.rapid7.com/blog/post/2021/07/21/microsoft-sam-file-readability-cve-2021-36934-what-you-need-to-know/

HiveNightmare aka SeriousSAM vulnerability : what to do
https://news.sophos.com/en-us/2021/07/22/hivenightmare-aka-serioussam-vulnerability-what-to-do/

Easily exploitable, unpatched Windows privilege escalation flaw revealed (CVE-2021-36934)
https://www.helpnetsecurity.com/2021/07/21/cve-2021-36934/