# CVE Detail – CVE-2021-36934

<p>An elevation of privilege vulnerability exists because of overly permissive Access Control Lists (ACLs) on multiple system files, including the Security Accounts Manager (SAM) database. An attacker who successfully exploited this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.</p>  
<p>An attacker must have the ability to execute code on a victim system to exploit this vulnerability.</p>  
<p>After installing this security update, you <em>must</em> manually delete all shadow copies of system files, including the SAM database, to fully mitigate this vulnerabilty. <strong>Simply installing this security update will not fully mitigate this vulnerability.</strong> See <a href="https://support.microsoft.com/topic/1ceaa637-aaa3-4b58-a48b-baf72a2fa9e7">KB5005357- Delete Volume Shadow Copies</a>.</p>

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.99536

## CVSS Scoring

CVSS v3.1 Score: 7.8

Severity: HIGH

## CISA KEV

KEV is present

## Affected Products

* cpe:2.3:o:microsoft:windows\_10\_1809:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:microsoft:windows\_10\_1909:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:microsoft:windows\_10\_2004:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:microsoft:windows\_10\_20h2:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:microsoft:windows\_10\_21h1:\*:\*:\*:\*:\*:\*:\*:\*