# CVE-2021-36942

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2021-36942 |
| **State** | PUBLIC |
| **Assigner** | secure@microsoft.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2021-08-12 18:15:00 UTC |
| **Updated** | 2023-12-28 20:15:00 UTC |
| **Description** | Windows LSA Spoofing Vulnerability |

## Risk And Classification

**EPSS:** 0.937270000 probability, percentile 0.998550000 (date 2026-05-17)

**CISA KEV:** Listed on 2021-11-03; due 2021-11-17; ransomware use Known

**Problem Types:** NVD-CWE-Other

## CISA Known Exploited Vulnerability

| | |
|---|---|
| **Vendor** | Microsoft |
| **Product** | Windows |
| **Name** | Microsoft Windows Local Security Authority (LSA) Spoofing Vulnerability |
| **Required Action** | Apply updates per vendor instructions. |
| **Notes** | https://nvd.nist.gov/vuln/detail/CVE-2021-36942 |

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Microsoft | Windows Server 2008 | - | sp2 | All | All |
| Operating System | Microsoft | Windows Server 2008 | r2 | sp1 | All | All |
| Operating System | Microsoft | Windows Server 2012 | - | All | All | All |
| Operating System | Microsoft | Windows Server 2012 | r2 | All | All | All |
| Operating System | Microsoft | Windows Server 2016 | - | All | All | All |
| Operating System | Microsoft | Windows Server 2016 | 2004 | All | All | All |
| Operating System | Microsoft | Windows Server 2016 | 20h2 | All | All | All |
| Operating System | Microsoft | Windows Server 2019 | - | All | All | All |

## References

| Reference | Sou |
| --- | --- |
| VU#405600 - Microsoft Windows Active Directory Certificate Services can allow for AD compromise via PetitPotam NTLM relay attacks | CER |
| Security Update Guide - Microsoft Security Response Center | N/A |
| CVE Program record | CVE |
| NVD vulnerability detail | NVD |
| CISA Known Exploited Vulnerabilities catalog | CIS |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

91803 Microsoft Windows Local Security Authority (LSA) Spoofing Vulnerability August 2021

91813 Microsoft Azure Stack Hub Security Updates - August 2021