# CVE Detail – CVE-2020-1472

An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC). An attacker who successfully exploited the vulnerability could run a specially crafted application on a device on the network.
To exploit the vulnerability, an unauthenticated attacker would be required to use MS-NRPC to connect to a domain controller to obtain domain administrator access.
Microsoft is addressing the vulnerability in a phased two-part rollout. These updates address the vulnerability by modifying how Netlogon handles the usage of Netlogon secure channels.
For guidelines on how to manage the changes required for this vulnerability and more information on the phased rollout, see How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472 (updated September 28, 2020).
When the second phase of Windows updates become available in Q1 2021, customers will be notified via a revision to this security vulnerability. If you wish to be notified when these updates are released, we recommend that you register for the security notifications mailer to be alerted of content changes to this advisory. See Microsoft Technical Security Notifications.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.9999

## CVSS Scoring

CVSS v3.1 Score: 5.5

Severity: MEDIUM

## CISA KEV

KEV is present

## Affected Products

* cpe:2.3:o:microsoft:windows\_server\_1903:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:microsoft:windows\_server\_1909:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:microsoft:windows\_server\_2004:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:microsoft:windows\_server\_2008:r2:sp1:\*:\*:\*:\*:x64:\*
* cpe:2.3:o:microsoft:windows\_server\_2012:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:microsoft:windows\_server\_2012:r2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:microsoft:windows\_server\_2016:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:microsoft:windows\_server\_2019:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:microsoft:windows\_server\_20h2:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:31:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:32:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:33:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:leap:15.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:leap:15.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:14.04:\*:\*:\*:esm:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:16.04:\*:\*:\*:esm:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:16.04:\*:\*:\*:lts:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:18.04:\*:\*:\*:lts:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:20.04:\*:\*:\*:lts:\*:\*:\*
* cpe:2.3:a:synology:directory\_server:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:samba:samba:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:samba:samba:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:samba:samba:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:9.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:zfs\_storage\_appliance\_kit:8.8:\*:\*:\*:\*:\*:\*:\*