

We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking “Manage Cookies” at the bottom of the page. [Privacy Statement](#) [Third-Party Cookies](#)


Accept

Reject

Manage cookies

[MSRC](#) > [Customer Guidance](#) > [Security Update Guide](#) > [Advisories](#) > **[CVE 2020 1472](#)**

## Netlogon Elevation of Privilege Vulnerability


On this page 

CVE-2020-1472  
Security Vulnerability

 [Subscribe](#)  [RSS](#)  [PowerShell](#)  [API](#)

**Released: Aug 11, 2020**  
**Last updated: Feb 11, 2021**

Assigning CNA: Microsoft

[CVE-2020-1472](#) 

Impact: Elevation of Privilege    Max Severity: Critical

CVSS:3.1 5.5 / 5.0 

 Expand all  Collapse all

Metric	Value
▼ Base score metrics (8)	
▶ Attack Vector	▶ Local
▶ Attack Complexity	▶ Low
▶ Privileges Required	▶ Low
▶ User Interaction	▶ None
▶ Scope	▶ Unchanged
▶ Confidentiality	▶ High
▶ Integrity	▶ None
▶ Availability	▶ None
▼ Temporal score metrics (3)	
▶ Exploit Code Maturity	▶ Proof-of-Concept
▶ Remediation Level	▶ Official Fix
▶ Report Confidence	▶ Confirmed

Please see [Common Vulnerability Scoring System](#) for more information on the definition of these metrics.

### Executive Summary

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](#)