CVE-2020-1472 | Netlogon Elevation of Privilege Vulnerability

Security Vulnerability

Published: 08/11/2020 | Last Updated : 08/11/2020
MITRE 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.

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.

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

FAQ

Do I need to take further steps to be protected from this vulnerability?
Yes. After installing the security updates released on August 11, 2020, you can deploy Domain Controller (DC) enforcement mode now or wait for the Q1 2021 update. See How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472 for more details.
If I install the updates and take no further action, what will be the impact?
During the initial deployment phase starting with the updates released August 11, 2020, the updates can be installed without added further action, and Windows devices and Domain Controllers (DCs) will be protected from this vulnerability. Organizations will need to monitor for and address potential issues before the Q1 2021 DC enforcement phase or risk devices being denied access. For more information, see How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472.

How does Microsoft plan to address this vulnerability?
Microsoft is addressing this vulnerability in a phased rollout. The initial deployment phase starts with the Windows updates released on August 11, 2020. The updates will enable the Domain Controllers (DCs) to protect Windows devices by default, log events for non-compliant device discovery, and have the option to enable protection for all domain-joined devices with explicit exceptions.

The second phase, planned for a Q1 2021 release, marks the transition into the enforcement phase. The DCs will be placed in enforcement mode, which requires all Windows and non-Windows devices to use secure Remote Procedure Call (RPC) with Netlogon secure channel or to explicitly allow the account by adding an exception for any non-compliant device.

What is a non-compliant device?
A non-compliant device is one that uses a vulnerable Netlogon secure channel connection.

Why is there a staged or phased rollout?
There are many non-Windows device implementations of the Netlogon Remote Protocol (also called MS-NRPC). To ensure that vendors of non-compliant implementations can provide customers with updates, a second release that is planned for Q1 2021 will enforce protection for all domain-joined devices.

Why do I need to follow the guidelines in How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472?
If the guidelines from the KB article are not followed, your organization risks devices in your environment being denied access when the enforcement phase starts in Q1 2021. If there are currently no non-compliant devices in your environment, you can move to enforcement mode for further protection in advance of required enforcement.

How can I be notified when the second release is available in Q1 2021?
When the second phase of Windows updates become available, 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.