



SECURITY BULLETIN – RESOURCE MANAGER AND NETLOGON'S ELEVATION OF PRIVILEGE VULNERABILITY

Advisory Version 1.0

DATE PUBLISHED: September 24th, 2020

ANY INFORMATION IN THIS ADVISORY IS SUBJECT TO CHANGE.

Please Note: This is a living document and may be subject to updates. The latest version of this document can be found at the following URL:

<https://support.polycom.com/content/support/security-center.html>

Summary

An elevation of privilege vulnerability exists in Netlogon when an attacker establishes a vulnerable Netlogon secure channel connection to a Microsoft Active Directory 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. As part of their response to this, Microsoft has disabled specific protocols which may be in use for some RPRM customers. For these customers an alternate configuration is needed to restore functionality.

For additional details please see publications from Microsoft and NVD for CVE information:

<https://support.microsoft.com/en-us/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc>

<https://nvd.nist.gov/vuln/detail/CVE-2020-1472>

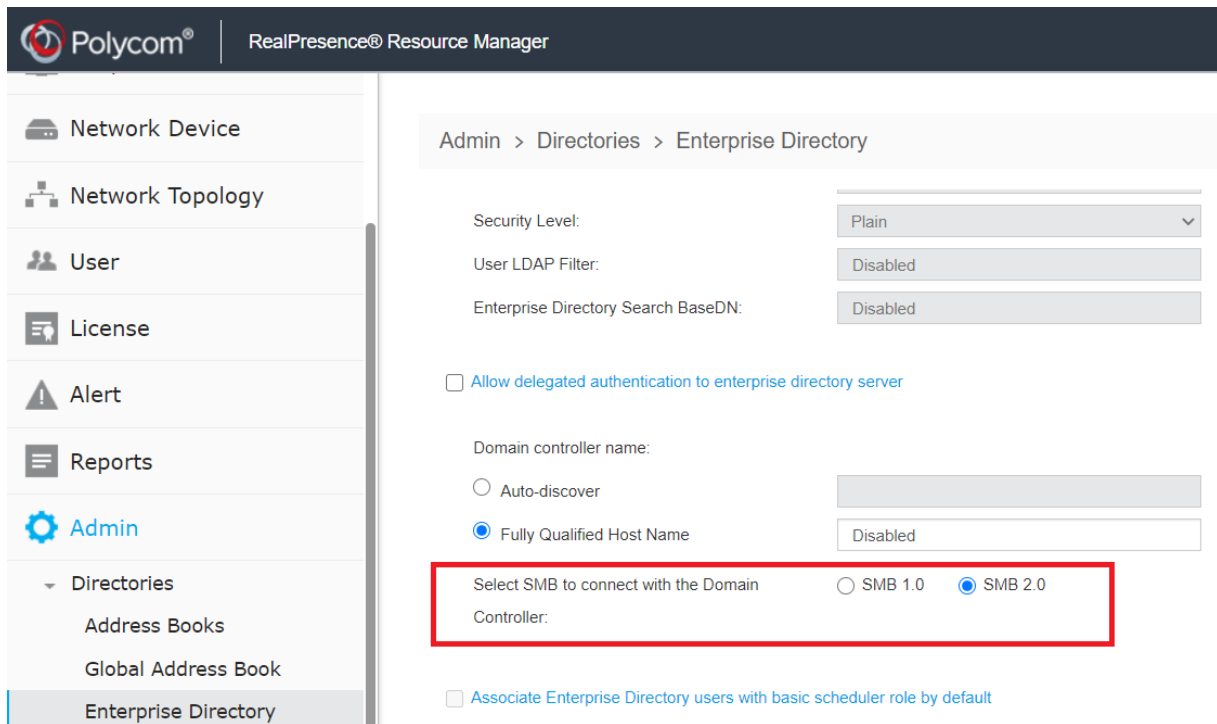
Solution

The RealPresence Resource Manager (RPRM) will continue to work when secure Netlogon is enabled in Microsoft Active Directory domain controller. In RPRM 10.3 or higher, from the Web UI, go to:

Admin -> Directories -> Enterprise Directory

Set "Select SMB to connect with the Domain Controller" field to **SMB 2.0** and Click Update.

Products running version older than 10.3 will need to upgrade to 10.3 or higher in order to set RPRM to use SMB 2.0 to connect to Domain Controller.



The Poly RealPresence Resource Manager software, release notes, and other documentation for your Poly and Plantronics headsets can be found at:

<https://support.polycom.com/content/support/north-america/usa/en/support/network/management-scheduling/realpresence-resource-manager.html>

CVSS v3 Base Metrics

To assist our customers in the evaluation of this vulnerability, Poly uses the Common Vulnerability Scoring System (CVSS). This system provides an open framework for communicating the characteristics and impacts of information technology vulnerabilities that better enable our customers to make informed decisions and assess the impact on their environment.

Base CVSS v3 Scores

CVE-2020-1472 CVSS 10 “Critical” CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H



Contact

Any customer using an affected system who is concerned about this vulnerability within their deployment should contact Polycom Technical Support – either call 1-800-POLYCOM or visit:

<https://support.polycom.com/content/support/security-center.html> For the latest information.

You might also find value in the high-level security guidance and security news located at:

<https://support.polycom.com/content/support/security-center.html>

Poly's Vulnerability Disclosure Policy can be found at:

<https://support.polycom.com/content/dam/polycom-support/global/documentation/product-vulnerability-disclosure-policy.pdf>

Revision History

Revision 1.0 - Original publication: September 24th, 2020

©2020 Plantronics, Inc. All rights reserved.

Trademarks

Poly, the propeller design, and the Poly logo are trademarks of Plantronics, Inc. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Poly.

Disclaimer

While Poly uses reasonable efforts to include accurate and up-to-date information in this document, Poly makes no warranties or representations as to its accuracy. Poly assumes no liability or responsibility for any typographical errors, out of date information, or any errors or omissions in the content of this document. Poly reserves the right to change or update this document at any time. Individuals are solely responsible for verifying that they have and are using the most recent Technical Bulletin.

Limitation of Liability

Poly and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Poly and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Poly has been advised of the possibility of such damages.

