Schneider Electric Security Bulletin

Netlogon Elevation of Privilege Vulnerability - Zerologon

13 October 2020

Overview

On August 11, 2020, Microsoft disclosed the Netlogon privilege escalation vulnerability, which affects Windows Servers and Samba Windows interoperability suite of programs for Linux and Unix.

According to the Microsoft advisory, the privilege escalation 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 exploits the vulnerability could run a specially crafted application on a network device.

Multiple exploits for this severe vulnerability are publicly available, and it is reportedly being exploited by nation-state threat actors.

Microsoft has released a first partial patch to mitigate the vulnerability. The second phase of the patch will be released in February 2021 to completely mitigate the vulnerability. Schneider Electric continues to assess how the vulnerability impacts our offers. In the meantime, customers should immediately make sure they have implemented cybersecurity best practices across their operations to protect themselves from the vulnerability. Where appropriate this includes locating your industrial systems and remotely accessible devices behind firewalls; installing physical controls to prevent unauthorized access; and preventing mission-critical systems and devices from being accessed from outside networks.

Please subscribe to the Schneider Electric security notification service to be informed of updates to this bulletin:

https://www.schneider-electric.com/en/work/support/cybersecurity/security-notifications.jsp

For additional information and support, please contact your Schneider Electric sales or service representative or Schneider Electric's Customer Care Center.

Details

The Netlogon vulnerability (CVE-2020-1472) is a protocol level flaw that allows privilege escalation. In September, Samba also disclosed that certain versions of their Linux interoperability library are vulnerable to CVE-2020-1472, depending on its configuration. Microsoft classified this vulnerability as critical, with a CVSS score of 10 and a temporal score of 9.0.

To exploit this vulnerability, the attacker would need to launch the attack from a machine on the same local network as their target. The attack requires that the spoofed login works like a normal domain login attempt. Active Directory (AD) would need to recognize the connecting client as being within its logical topology, which external addresses wouldn't have.

Microsoft has reported increased activities leveraging the Zerologon exploit, including from nation-state threat actors.

Recommended Mitigations

Schneider Electric continues to monitor and track research into these vulnerabilities to determine appropriate actions to be taken. Customers should follow any existing product specific support policies or guidance provided by Schneider Electric.

Via its advisory, Microsoft has provided recommendations to protect users' environments and prevent outages. Please note that as of the date of this publication, it is unclear how Microsoft's patch and other recommendations will affect systems performance.

We advise customers to refer immediately to Microsoft's security update and resources for further information and guidance.

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and networks.
- Place all controllers in locked cabinets and never leave them in the "Program" mode.
- Never connect programming software to any network other than the network for the devices that it is intended for.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.
- Never allow mobile devices that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and systems, and ensure that they are not accessible from the Internet.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

Refer to the Schneider Electric Recommended Cybersecurity Best Practices document for more details.

Schneider Electric Security Bulletin

For More Information

This document provides an overview of the identified vulnerability or vulnerabilities and actions required to mitigate. For more details and assistance on how to protect your installation, contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

https://www.se.com/ww/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

LEGAL DISCLAIMER

THIS NOTIFICATION DOCUMENT, THE INFORMATION CONTAINED HEREIN, AND ANY MATERIALS LINKED FROM IT (COLLECTIVELY, THIS "NOTIFICATION") ARE INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND SUGGESTED MITIGATION ACTIONS, REMEDIATION, FIX, AND/OR GENERAL SECURITY RECOMMENDATIONS AND IS PROVIDED ON AN "AS-IS" BASIS WITHOUT WARRANTY OR GUARANTEE OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES RELATING TO THIS NOTIFICATION, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SCHNEIDER ELECTRIC MAKES NO WARRANTY THAT THE NOTIFICATION WILL RESOLVE THE IDENTIFIED SITUATION. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES OR LOSSES WHATSOEVER IN CONNECTION WITH THIS NOTIFICATION, INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOUR USE OF THIS NOTIFICATION IS AT YOUR OWN RISK, AND YOU ARE SOLELY LIABLE FOR ANY DAMAGES TO YOUR SYSTEMS OR ASSETS OR OTHER LOSSES THAT MAY RESULT FROM YOUR USE OF THIS NOTIFICATION. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION.

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and automation digital** solutions for **efficiency and sustainability.** We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Schneider Electric Security Bulletin

Revision Control:

Version 1 *13 October 2020*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2020.10.12 09:18:58 -04'00'