Schneider Electric Security Bulletin

BadAlloc Vulnerabilities

19 August 2021

Overview

Schneider Electric is aware of multiple memory allocation vulnerabilities dubbed ‘BadAlloc’, disclosed by Microsoft on April 29, 2021. Full details of the BadAlloc vulnerabilities can be found in the ICS-CERT Advisory (ICSA-21-119-04). Schneider Electric continues to monitor and track research into the BadAlloc vulnerabilities to determine appropriate actions to be taken.

Customers should ensure they have implemented cybersecurity best practices across their operations to protect themselves from possible exploitation of these vulnerabilities. Where appropriate, this includes locating their industrial systems and remotely accessible devices behind firewalls; installing physical controls to prevent unauthorized access; preventing mission-critical systems and devices from being accessed from outside networks; and following the general security recommendations below.

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

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

Microsoft’s Section 52 security research group disclosed over twenty-five vulnerabilities which affects a wide range of domains including industrial control systems, Industrial IoT, medical IoT and Operational Technology (OT). According to Microsoft, the vulnerabilities exist in standard memory allocation functions used widely in real-time operating systems (RTOS).

Additionally, Blackberry recently disclosed that its QNX operating system which is widely used in embedded systems is also impacted by the memory allocation bugs. It is tracked as CVE-2021-22156, the complete list of affected real-time operating systems can be found in the advisory released by US-CERT: ICS-CERT Advisory (ICSA-21-119-04).

Recommended Mitigations

Schneider Electric continues to assess how the BadAlloc vulnerabilities affect its offers, and will update customers through its Cybersecurity Support Portal as additional product-specific information becomes available.

The ICS-CERT Advisory (ICSA-21-119-04) provides links to specific vendor advisories to protect users’ environments and prevent outages. Please note that as of the date of this publication, it is unclear how the different patches and other recommendations will affect system performance.

Schneider Electric Security Bulletin

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 intended for that device.
- 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.

For more information refer to the Schneider Electric Recommended Cybersecurity Best Practices document.

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, please 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

Revision Control:

Version 1 *19 August 2021*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2021.08.18 20:42:01 -04'00'