Schneider Electric Security Notification

C-Bus Toolkit and C-Gate Server

13 April 2021 (08 November 2022)

Overview

Schneider Electric is aware of multiple vulnerabilities in its C-Bus Toolkit and C-Gate server products.

The C-Bus Toolkit product, which includes C-Gate Server, is an application you run on your personal computer to configure and commission C-Bus Installations.

Failure to apply the remediations provided below may risk remote code execution attack, which could result in an attacker having remote access to the computer.

November 2022 Update: The CWE for CVE-2021-22716 has been updated (marked in red). No additional action is required for customers who have already followed the remediation instructions provided below.

Affected Product and Versions

	CVE-						
	2021-22716	2021-22717	2021-22718	2021-22719	2021-22720	2021-22748	2021-22796
C-Bus Toolkit V1.15.9 and prior	X	X	X	X	X	X	
C-Gate Server 2.11.7 and prior					X		X

Vulnerability Details

CVE ID: **CVE-2021-22717**

CVSS v3.0 Base Score 8.8 | High | CVSS:3.0/ AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

A *CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')* vulnerability exists that could allow a remote code execution when processing config files.

CVE ID: **CVE-2021-22719**

CVSS v3.0 Base Score 8.8 | High | CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

A *CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')* vulnerability exists that could allow a remote code execution when a file is uploaded.

CVE ID: **CVE-2021-22748**

CVSS v3.1 Base Score 8.8 | High | CVSS:3.1/ AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

A *CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')* vulnerability exists that could allow a remote code execution when a file is saved.

CVE ID: **CVE-2021-22796**

CVSS v3.1 Base Score 8.8 | High | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

A *CWE-287: Improper Authentication* vulnerability exists that could allow remote code execution when a malicious file is uploaded.

CVE ID: **CVE-2021-22716**

CVSS v3.0 Base Score 7.8 | High | CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

A *CWE-732: Incorrect Permission Assignment for Critical Resource* vulnerability exists that could allow remote code execution when an unprivileged user modifies a file.

CVE ID: **CVE-2021-22718**

CVSS v3.0 Base Score 7.8 | High | CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

A *CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')* vulnerability exists that could allow a remote code execution when restoring project files.

CVE ID: **CVE-2021-22720**

CVSS v3.0 Base Score 6.5 | Medium | CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

A *CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')* vulnerability exists that could allow a remote code execution when restoring a project.

Remediation

Affected Product & Versions	Remediation
C-Bus Toolkit *V1.15.9 and prior*	Version 1.15.10 of the C-Bus Toolkit product, which contains the C-Gate Server, includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/product-range/2216-spacelogic-c-bus-home-automation-system/?parent-subcategory-id=88010&filter=business-5-residential-and-small-business----software-firmware-tab#software-and-firmware A reboot will be needed after the update.
C-Gate Server *V2.11.7 and prior*	Version 2.11.8 of the C-Gate Server product, includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/product-range/2216-spacelogic-c-bus-home-automation-system/?parent-subcategory-id=88010&filter=business-5-residential-and-small-business----software-firmware-tab#software-and-firmware A reboot will be needed after the update.

Customers should use appropriate patching methodologies when applying these patches to their systems. We strongly recommend the use of back-ups and evaluating the impact of these patches in a Test and Development environment or on an offline infrastructure. Contact Schneider Electric's Customer Care Center if you need assistance removing a patch.

If customers choose not to apply the remediation provided above, they should immediately apply the following mitigations to reduce the risk of exploit:

- Use an allow list for this this application
- Turn on the computer's firewall
- Use an antivirus program
- Secure this computer to prevent unauthorized personnel from accessing this computer

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.

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

Acknowledgements

Schneider Electric recognizes the following researchers for identifying and helping to coordinate a response to these vulnerabilities:

CVE	Researchers
CVE-2021-22716	Simon Zuckerbraun of Trend Micro Zero Day Initiative
CVE-2021-22717, CVE-2021-22718, CVE-2021-22719	rgod working with Trend Micro Zero Day Initiative
CVE-2021-22720	rgod working with Trend Micro Zero Day Initiative & Tenable Security
CVE-2021-22796	Tenable Security

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: https://www.se.com/ww/en/work/solutions/cybersecurity/. These organizations will be fully aware of this situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric’s products, visit the company’s cybersecurity support portal page:
https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

LEGAL DISCLAIMER

Schneider Electric Security Notification

About Schneider Electric

Schneider's purpose is to empower all to make the most of our energy and resources, bridging progress and sustainability for all. We call this Life Is On.

Our mission is to be your digital partner for Sustainability and Efficiency.

We drive digital transformation by integrating world-leading process and energy technologies, end-point to cloud connecting products, controls, software and services, across the entire lifecycle, enabling integrated company management, for homes, buildings, data centers, infrastructure and industries.

We are the most local of global companies. We are advocates of open standards and partnership ecosystems that are passionate about our shared Meaningful Purpose, Inclusive and Empowered values.
www.se.com

Revision Control:

Version 1.0 *13 April 2021*	Original Release
Version 2.0 *08 June 2021*	Added CVE-2021-22748
Version 3.0 *14 September 2021*	• C-Gate Server added as an affected product of CVE-2021-22720 • CVE-2021-22796 added • Updated the previously provided remediation • Added Tenable Security to the acknowledgement section
Version 4.0 *08 November 2022*	The CWE for CVE-2021-22716 has been updated (marked in red). No additional action is required for customers who have already followed the remediation instructions provided below.

Product Security Office

Digitally signed by Product Security Office
Date: 2022.11.09 16:47:35 -05'00'