Schneider Electric Security Notification

Conext™ Combox

14 June 2022

Overview

Schneider Electric is aware of multiple vulnerabilities in its Conext™ ComBox product which was discontinued in January 2020 and is no longer in support.

The Conext™ ComBox is a communication and monitoring device for installers and operators of Conext solar systems. It features an integrated web server, enabling graphical displays of system daily, monthly and lifetime energy data to be viewed using a simple web browser or Android tablet device.

Failure to apply the mitigations provided below may risk Clickjacking, Rate Limiting & Cross-Site Request Forgery attacks. An attacker who successfully exploits one or more of these vulnerabilities could trick the product user/admin into performing unintended actions that may lead to taking over their account or manipulating the station settings.

Affected Product and Versions

Product	Version
Conext™ ComBox	All Versions

Vulnerability Details

CVE ID: **CVE-2022-32515**

CVSS v3.1 Base Score 8.6 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

A *CWE-307: Improper Restriction of Excessive Authentication Attempts* vulnerability exists that could cause brute force attacks to take over the admin account when the product does not implement a rate limit mechanism on the admin authentication form.

CVE ID: **CVE-2022-32516**
CVSS v3.1 Base Score 7.5 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A *CWE-352: Cross-Site Request Forgery (CSRF)* vulnerability exists that could cause system's configurations override and cause a reboot loop when the product suffers from POST-Based Cross-Site Request Forgery (CSRF).

CVE ID: **CVE-2022-32517**
CVSS v3.1 Base Score 6.5 | Medium | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

A *CWE-1021: Improper Restriction of Rendered UI Layers or Frames* vulnerability exists that could cause an adversary to trick the interface user/admin into interacting with the application in an unintended way when the product does not implement restrictions on the ability to render within frames on external addresses.

Schneider Electric Security Notification

Mitigation

Affected Product & Version	Mitigations
Conext™ ComBox *All Versions*	Conext™ ComBox product was discontinued as of January 2020 and is no longer in support. Customers should immediately apply the following mitigations to reduce the risk of exploit: • Do not expose the Conext™ Combox directly to the Internet • Do not grant network access to unknown computers • Computer(s) must be kept up to date with the latest security patches Customers should also consider upgrading to the latest product offering InsightHome & InsightFacility to resolve these issues.

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.

Schneider Electric Security Notification

Acknowledgement

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

CVE	Researcher
CVE-2022-32515, CVE-2022-32516, CVE-2022-32517	Tony Marcel Nasr

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

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.

Schneider Electric Security Notification

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 *14 June 2022*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2022.06.13 11:28:30 -04'00'