

# Schneider Electric Security Notification

## SAGE RTU

11 June 2024

### Overview

Schneider Electric is aware of multiple vulnerabilities in its SAGE RTU products.

The [SAGE RTU](#) products are hardware devices that collect utility substation information from different devices and passes it along to a SCADA software platform.

Failure to apply the remediation provided below may risk total compromise of the impacted device, leading to loss of data, loss of operation, or impacts to the performance of the device.

### Affected Products and Versions

Product	Version
Sage 1410 Sage 1430 Sage 1450 Sage 2400 Sage 3030 Magnum Sage 4400	Versions C3414-500-S02K5_P8 and prior

### Vulnerability Details

CVE ID: **CVE-2024-37036**

CVSS v3.1 Base Score 9.8 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

*CWE-787: Out-of-bounds Write* vulnerability exists that could result in an authentication bypass when sending a malformed POST request and particular configuration parameters are set.

CVE ID: **CVE-2024-37037**

CVSS v3.1 Base Score 8.1 | High | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

*CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')* vulnerability exists that could allow an authenticated user with access to the device's web interface to corrupt files and impact device functionality when sending a crafted HTTP request.

CVE ID: **CVE-2024-37038**

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

*CWE-276: Incorrect Default Permissions* vulnerability exists that could allow an authenticated user with access to the device's web interface to perform unauthorized file and firmware uploads when crafting custom web requests.

## Schneider Electric Security Notification

**CVE ID: CVE-2024-37039**

CVSS v3.1 Base Score 5.9 | Medium | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

*CWE-252: Unchecked Return Value* vulnerability exists that could cause denial of service of the device when an attacker sends a specially crafted HTTP request.

**CVE ID: CVE-2024-37040**

CVSS v3.1 Base Score 5.4 | Medium | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L

*CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')* vulnerability exists that could allow a user with access to the device's web interface to cause a fault on the device when sending a malformed HTTP request.

**CVE ID: CVE-2024-5560**

CVSS v3.1 Base Score 5.3 | Medium | CVSS:3.1/ AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

*CWE-125: Out-of-bounds Read* vulnerability exists that could cause denial of service of the device's web interface when an attacker sends a specially crafted HTTP request.

*Note regarding vulnerability details: The severity of vulnerabilities was calculated using the CVSS Base metrics in version 3.1 ([CVSS v3.1](#)) without incorporating the Temporal and Environmental metrics. Schneider Electric recommends that customers score the CVSS Environmental metrics, which are specific to end-user organizations, and consider factors such as the presence of mitigations in that environment. Environmental metrics may refine the relative severity posed by the vulnerabilities described in this document within a customer's environment.*

### Remediation

Affected Product & Version	Remediation
<b>Sage 1410</b> <b>Sage 1430</b> <b>Sage 1450</b> <b>Sage 2400</b> <b>Sage 3030 Magnum</b> <b>Sage 4400</b>  <i>Versions C3414-500-S02K5_P8 and prior</i>	Firmware version C3414-500-S02K5_P9 of SAGE RTU includes a fix for these vulnerabilities and is available on request from Schneider Electric's Customer Care Center: <a href="https://www.se.com/ww/en/work/support/">https://www.se.com/ww/en/work/support/</a>

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

## Schneider Electric Security Notification

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.

### 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.

### Acknowledgements

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

CVE	Researchers
CVE-2024-37036	Marlon Schumacher, LLNL
CVE-2024-37037 CVE-2024-37039 CVE-2024-37040	Alex Armstrong, LLNL
CVE-2024-5560 CVE-2024-37038	Vishal Madipadga, SNL

# Schneider Electric Security Notification

## 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

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

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](http://www.se.com)

# Schneider Electric Security Notification

Revision Control:

<b>Version 1.0.0</b> <i>11 June 2024</i>	Original Release
---	------------------