



NPCC Security Bulletin

TLP: WHITE

March 3, 2022

NPCC is publishing this security bulletin to engage and inform NPCC entities on aspects of Bulk Power System security and reliability.

CISA Advisory

Schneider Electric Easergy P5 and P3 Hard-coded Credentials and Classic Buffer Overflow Vulnerabilities

CISA issued ICS Advisory (ICSA-22-055-03) on February 24, 2022 regarding Schneider Electric Easergy P5 and P3 Hard-coded Credentials and Classic Buffer Overflow vulnerabilities. Successful exploitation of these vulnerabilities may disclose device credentials, cause a denial-of-service condition, program crashes and arbitrary code execution, device reboot, or allow an attacker to gain full control of the relay. This could result in loss of protection to the electrical network.

Schneider Electric recommends users using Easergy P5 to upgrade to **version 01.401.101** and users using Easergy P3 to upgrade to **version 30.205** and follow industry cybersecurity best practices. If users choose not to apply the updated versions, they should immediately disable the GOOSE service of the product to reduce the risk of exposure. If GOOSE is needed for the application, use it only in a secure local area network.

CISA Advisory: [ICS Advisory \(ICSA-22-055-03\) Schneider Electric Easergy P5 and P3](#)

CISA Best Practices: [Control Systems Security Recommended Practices](#)

CISA's Defense Strategies: [Improving ICS Cybersecurity with Defense-in-Depth Strategies](#)

Schneider Electric's Security Notifications: [SEVD-2022-011-03](#), [SEVD-2022-011-04](#)

Schneider Electric Best Practices: [Recommended Cybersecurity Best Practices](#)

NPCC assumes no responsibility for any material, e.g., information, data, text, software, graphics et cetera, of computer "links" to sites hosted by third parties that are outside of NPCC's control. NPCC does not endorse products, services, or information provided by third parties and shall not be responsible or liable, directly, or indirectly, for any damage or loss caused or alleged to be caused by or in connection with, use or reliance on any content available on or through any third-party site. Further, the inclusion of links to third party websites within this Security Bulletin does not imply that the owners of such third party websites have given permission for inclusion of these links, or otherwise sponsored or endorsed NPCC's Security Bulletin.

NPCC is not responsible for the accessibility of third party websites via the Security Bulletin. Should you discover that a third party link on a Security Bulletin is broken, no longer pointing to the content so indicated on the Security Bulletin, or points to a third party website containing infringing content, malicious code, or any offensive, libelous, or otherwise illegal or inappropriate content, email: support@npcc.org. To ensure NPCC can quickly respond to the issue, your email should include the originating Security Bulletin, the linked page URL and a description of the content in question.