Improper authentication handling for Digi PortServer TS; Digi One SP, SP IA, IA; Digi One IAP

Digi International has identified a security vulnerability affecting all versions of these products running firmware with release dates prior to 2025:

- **PortServer TS**
- **Digi One SP/Digi One SP IA/Digi One IA**
- **Digi One IAP**

We are committed to the security and integrity of our products and the safety of our customers. Upon discovery of this issue, our engineering team initiated a full investigation and has developed a fix to address the vulnerability.

CVE Identifier

This vulnerability is tracked under the following CVE ID: **CVE-2025-3659**. Full details can be found in the https://nvd.nist.gov/vuln/detail/CVE-2025-3659.

What You Should Do

We strongly recommend that all customers update their devices to the latest firmware version as soon as possible to mitigate any potential security risks. Firmware updates and instructions can be found at:

- PortServer TS Support Page
- Digi One SP/ Digi One SP IA/ Digi One IA support page
- Digi One IAP Support Page

Recommended Actions:

1. Review the affected product(s) in your environment.
2. Download and apply the latest firmware update.
3. **If you cannot update at this time**, we recommend the following mitigation:
   - Disable the web server when not configuring the device.

Support and Questions

If you have any questions or require assistance, please contact our support team: https://www.digi.com/support.

We appreciate your attention to this matter and thank you for your continued trust in Digi International.