Security Advisory: Incorrect Authorization

Overview

Digi International has identified a security vulnerability affecting the following products running any firmware released in 2025 or earlier affecting the Digi PortServer TS, Digi One SP, Digi One SP IA, and Digi One IA. This vulnerability allows an unauthenticated actor to bypass authentication and gain access to restricted resources on the device.

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 identified mitigations to address the vulnerability.

Vulnerability Details

This vulnerability allows an unauthenticated actor to bypass authentication and gain access to restricted resources on the device.

CVE Identifier

This vulnerability is tracked under the following CVE ID: **CVE-2026-12352**. Full details can be found in the https://nvd.nist.gov/vuln/detail/CVE-2026-12352.

Affected Products

The following products are affected by this vulnerability when running firmware with a release date prior to 2025:

- Digi PortServer TS — all firmware versions prior to 2025
- Digi One SP — all firmware versions prior to 2025
- Digi One SP IA — all firmware versions prior to 2025
- Digi One IA — all firmware versions prior to 2025

What You Should Do

We strongly recommend that all customers apply the appropriate mitigation for their device as soon as possible to reduce exposure to this vulnerability. While the mitigations above will reduce exposure, we recommend upgrading to the **Digi Connect EZ** or **Digi Connect EZ TS** as a long-term solution. The Digi Connect EZ and Digi Connect EZ TS are the modern replacements for these products and address the underlying security limitations of the affected devices.

Recommended Actions:

1. Review the affected product(s) in your environment.
2. Apply the mitigation appropriate for your device as described below.

Digi PortServer TS:

- Enable HTTPS on the web server (recommended).
- Alternatively, disable the web server when it is not actively being used for configuration.
- **Compensating control:** If you cannot apply the HTTPS configuration, restrict access via firewall or VPN.

Digi One SP / Digi One SP IA / Digi One IA:

- Disable the web server.
- **Compensating control:** If you cannot apply the HTTPS configuration, restrict access via firewall or VPN.

Support and Questions

If you have any questions or require assistance, please contact our support team at https://www.digi.com/support. We appreciate your attention to this matter and thank you for your continued trust in Digi International.