# Security Advisory: Stored Cross-Site Scripting (XSS)

**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.

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:**

A stored cross-site scripting (XSS) vulnerability in the web management interface of the Digi PortServer TS, Digi One SP, Digi One SP IA, and Digi One IA allows a remote, authenticated administrator to inject script into certain system configuration fields. The script subsequently executes in the browser of a user who views the affected pages (CWE-79).

**CVE Identifier:**

This vulnerability is tracked under the following CVE ID: **CVE-2026-12948**. Full details can be found in the https://nvd.nist.gov/vuln/detail/CVE-2026-12948.

**Affected Products**

The following products are affected by this vulnerability:

- Digi PortServer TS — all firmware versions
- Digi One SP — all firmware versions
- Digi One SP IA — all firmware versions
- Digi One IA — all firmware versions

**Recommended Actions:**

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

No firmware fix will be issued for this product, which is approaching end-of-life. The following deployment practices are the recommended means of reducing exposure:

- Deploy the device on a trusted network segment, not exposed to untrusted or public networks.

- Place the device behind a firewall or VPN and restrict access to the web management interface to trusted administrative hosts only.
- Safeguard administrator credentials, since exploitation requires authenticated administrator access to write the affected fields.

**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. We also recommend updating firmware to the latest version. 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.

**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.