

Security Advisory: OS Command Injection in Digi Accelerated Linux (DAL OS) Web Administration Service

Overview

Digi International has identified a security vulnerability affecting Digi products running DAL OS versions 21.8.24.139 through 26.7.90.14, inclusive.

Our engineering and security teams have identified mitigation steps to address the vulnerability while official patches are being released.

Vulnerability Details

A specifically crafted HTTP POST request to the web administration interface allows an unauthenticated attacker to execute arbitrary operating system commands with root privileges on the affected device.

CVE Identifier

This vulnerability is tracked under the following CVE ID: CVE-2026-75937. Full details can be found in the <https://nvd.nist.gov/vuln/detail/CVE-2026-75937>.

CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H - **9.4 (Critical)**

Attack Vector is scored as Adjacent because the device's default configuration restricts web administration access to clients on the device's local LAN subnet. Customers who have modified this restriction to permit access from other subnets or from the WAN should evaluate whether Attack Vector is Network (CVSS 10.0) for their deployment and should prioritize mitigation and patching accordingly.

Affected Products

Digi products running DAL OS versions: 21.8.24.139 through 26.7.90.14, inclusive, are affected.

Device Family	Affected Versions	Patched Version #	Patch Release Date
Connect IT 4	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.2.148.166 - LTS Patch Release and 26.7.90.15 - Feature Firmware	24 Aug 2026

		Release	
Connect IT Mini	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.2.148.166 - LTS Patch Release and 26.7.90.15 - Feature Firmware Release	24 Aug 2026
Digi EX12	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.2.148.166 - LTS Patch Release and 26.7.90.15 - Feature Firmware Release	24 Aug 2026
Digi EX15	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.2.148.166 - LTS Patch Release and 26.7.90.15 - Feature Firmware Release	24 Aug 2026
Digi EX50	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.2.148.166 - LTS Patch Release and 26.7.90.15 - Feature Firmware Release	24 Aug 2026
Digi IX10	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.2.148.166 - LTS Patch Release and 26.7.90.15 - Feature Firmware Release	24 Aug 2026

Digi IX20	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.2.148.166 - LTS Patch Release and 26.7.90.15 - Feature Firmware Release	24 Aug 2026
Digi IX25	Vulnerable versions: 26.2.147.55 - 26.2.147.125	Patched in: 26.7.90.15	17 Aug 2026
Digi IX30	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.2.148.166 - LTS Patch Release and 26.7.90.15 - Feature Firmware Release	24 Aug 2026
Digi IX40	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.2.148.166 - LTS Patch Release and 26.7.90.15 - Feature Firmware Release	24 Aug 2026
Digi TX40	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.2.148.166 - LTS Patch Release and 26.7.90.15 - Feature Firmware Release	24 Aug 2026
Digi TX54	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.2.148.166 - LTS Patch Release	24 Aug 2026

		and 26.7.90.15 - Feature Firmware Release	
Digi TX64	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.2.148.166 - LTS Patch Release and 26.7.90.15 - Feature Firmware Release	24 Aug 2026
Digi TX65	Vulnerable versions: <i>no production firmware's available pre-26.8.3.24</i>	Patched in: 26.8.3.24	17 Aug 2026
Anywhere USB 2 Plus	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.2.148.166 – LTS Patch Release	2 Sept 2026
Anywhere USB 8 Plus	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.2.148.166 – LTS Patch Release	2 Sept 2026
Anywhere USB 8 Plus w/ WIFI	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.2.148.166 – LTS Patch Release	2 Sept 2026
Anywhere USB 24 Plus	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.2.148.166 – LTS Patch Release	2 Sept 2026
Anywhere USB 24 Plus w/ WIFI	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.2.148.166 – LTS Patch Release	2 Sept 2026

Connect EZ Mini/2/4	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.2.148.166 – LTS Patch Release	2 Sept 2026
Connect EZ 8	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.2.148.166 – LTS Patch Release	2 Sept 2026
Connect EZ 16/32	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.2.148.166 – LTS Patch Release	2 Sept 2026
Connect EZ 4 WS Connect EZ 04- WS00	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.2.148.166 – LTS Patch Release	2 Sept 2026
Connect IT 48	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.2.148.166 – LTS Patch Release	2 Sept 2026
Connect IT 16	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.2.148.166 – LTS Patch Release	2 Sept 2026
XBee Hive Gateway	Vulnerable versions: 25.8.138.60 - 26.7.90.14	Patched in: 26.9.10.28	2 Oct 2026
XBee Hive Border Router for Wi-SUN	Vulnerable versions: 25.8.138.60 - 26.7.90.14	Patched in: 26.9.10.28	2 Oct 2026
IX15 IoT Gateway & Cellular Router	Vulnerable versions: 21.8.24.139 - 26.7.90.14	Patched in: 26.9.10.28	2 Oct 2026
Digi 54xx Family	Vulnerable version: 21.8.24.139	Product is EOL and does not receive patches; follow	n/a

		mitigation steps below	
Digi 63xx Family	Vulnerable versions: 21.8.24.139 - 22.5.50.66	Product is EOL and does not receive patches; follow mitigation steps below	n/a
Digi IX14	Vulnerable versions: 21.8.24.139 - 22.5.50.62	Product is EOL and does not receive patches; follow mitigation steps below	n/a
Digi LR54 Family	Vulnerable versions: 21.8.24.139 - 23.12.1.56	Product is EOL and does not receive patches; follow mitigation steps below	n/a

Mitigations:

Until patches are released, we recommend the following mitigation steps to reduce risk:

Disable the web server when not configuring the device. You can do this by:

1. CLI via SSH:

- a. Log into the device through a terminal with admin credentials
- b. After login select the “Admin CLI”
- c. Run the following commands to disable the WebUI service:
 - i. `> config`
 - ii. `(config)> service web_admin enable false`
 - iii. `(config)> save`

2. Digi Remote Manager:

- a. Log into Digi Remote Manager
- a. Obtain the device configuration:
 - i. Inside of DigiRM: find your device, select the **Device ID**, select **Settings**, then expand the **Config**

i. Inside of the Local Web UI: Go to the menu and select **System**. Underneath the Configuration section, select **Device Configuration**

3. Once you are in the device configuration, select **Services** → **Web Administration**

4. Deselect **Enable**

5. Select **Apply** to save the configuration and apply the change

Note: If the device is managed by a Digi Remote Manager template (Configuration), disabling the web administration service on the device alone may not persist. Digi Remote Manager periodically checks each device against its template and may re-apply the template's settings if they don't match, which could turn the service back on. To make the change permanent, disable the web administration service in the template as well.

What You Should Do

- Apply the mitigation above until the official patch is available.
- Update affected devices as soon as it is released. Firmware is available at <https://remotemanager.digi.com/ui/login>
- After updating, change the administrator's password on all affected devices. If those credentials were reused on any other system, change them there as well.
- Review your device access control list settings. Devices configured to permit web administration access from outside the local LAN subnet are at increased risk and should be prioritized.

Acknowledgment

Digi International thanks 美团众包骑手:键盘手欧多克 for reporting this issue and for coordinating disclosure with us.

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.