



## Security Announcement

Announcement > SAP10505

### (Non-US) DI-8003: All Hardware Revisions / All Firmware Versions : End-of-Life (EoL) / End-of-Service (EoS) : Vulnerabilities Reported

**Publication ID:** SAP10505

**Resolved Status:** Yes

**Published on:** 15 April 2026 3:03 GMT

**Last updated on:** 15 April 2026 3:03 GMT

#### Overview

The DI-8003, all hardware revisions, have reached their End of Life ("EOL") / End of Service Life ("EOS") Life-Cycle. D-Link US recommends D-Link devices that have reached EOL/EOS, to be retired and replaced. Please contact your regional office for recommendations ([DI-8003 Record LINK](#)).

As a general policy, when products reach EOS/EOL, they can no longer be supported, and all firmware development for these products cease. **Please read information and recommendations below.**

#### Affected Models

Model	Region	Hardware Revision	End of Support	Legacy Website	Last Updated
DI-8003	Worldwide	All Series H/W Revisions	02/10/2021	<a href="#">Non-US Link</a>	04/14/2026

#### Recommendation for End of Support /End of Life Products

From time to time, D-Link will decide that some of its products have reached End of Support ("EOS") / End of Life ("EOL"). D-Link may choose to EOS/EOL a product due to the evolution of technology, market demands, new innovations, product efficiencies based on the latest technologies, or the product's maturity over time, which necessitates replacement with functionally superior technology.

#### For US Consumer

If a product has reached End of Support ("EOS") / End of Life ("EOL"), there is usually no further extended support or development for it.

Typically for these products, D-Link will be unable to resolve device or firmware issues since all development and customer support has ceased.

**D-Link strongly recommends that this product be retired and cautions that any further use of this product may be a risk to devices connected to it. If US consumers continue to use these devices against D-Link's recommendation, please ensure the device has the most recent firmware, update its unique password frequently to access its web-configuration, and always enable WIFI encryption with a unique password.**