



PRODUCT SECURITY ADVISORY

October 6, 2026

PSIRT Record Number
TEK-PSA-003-102026

OVERVIEW

The following vulnerability affects 6 Series B MSO devices with firmware versions v2.24.4 and v2.26.13.

- LXIToClientCommunicator HTTP API endpoint is vulnerable to shell injection. Command injected is executed as root bypassing the root user/guest user separation boundary.

PSIRT STATEMENT

The vulnerability identified is fixed in firmware version v2.28.18.

As of the date of this advisory, we are not aware of any reports of active exploitation.

Tektronix has requested CVE IDs for these vulnerabilities, but they have not yet been assigned by the CVE Numbering Authority. Once assigned, they will be added to this advisory.

ABOUT TEKTRONIX PRODUCT SECURITY

Tektronix helps our customers innovate solutions accurately, safely, and securely. Tektronix is committed to developing secure solutions for our customers.

The Product Security Incident Response Team (PSIRT) focuses on identifying, assessing, and analyzing risks associated with security vulnerabilities within Tektronix products. The Tektronix PSIRT is a diverse team of subject matter experts responsible for delivering best in class support to contain and minimize the vulnerability impact.

For more information about Tektronix Product Security and PSIRT, please visit us at <https://tek.com/en/support/product-security/advisories>

You may also contact us at PSIRT@tektronix.com.

Credit to Ermes Pennucci @ Janaralab, Unisannio for identifying and reporting this vulnerability

Initial Publication Date	Last Published Date
[10/6/2026]	[10/6/2026]