



PRODUCT SECURITY ADVISORY

September 15, 2026

PSIRT Record Number
TEK-PSA-002-092026

OVERVIEW

The following vulnerabilities affect 3 Series MDO devices with firmware version v1.19.13.

- An OS command injection vulnerability exists in the FILESystem:MOUNT:DRive SCPI command handler. Insufficient neutralization of user-supplied input may allow remote attackers to execute arbitrary operating system commands with elevated privileges.
- A path traversal vulnerability in the SCPI FILESystem command interface may allow remote attackers to read or modify arbitrary files on the device through insufficient validation of file paths supplied to filesystem access commands.
- A path traversal vulnerability exists in the web management interface of the device. Insufficient validation of user-supplied file paths may allow remote attackers to read arbitrary files accessible to the application. Depending on configuration, exploitation may be possible without authentication.

PSIRT STATEMENT

The vulnerabilities identified are fixed in firmware version v1.21.1.

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
[9/15/2026]	[9/17/2026]