VIVOTEK
A Delta Group Company

VIVOTEK Product Security Advisory

Advisory ID: VVTK-SA-20260701

CVE ID: CVE-2026-6682, CVE-2026-6683, CVE-2026-6684, CVE-2026-6685, CVE-2026-6686, CVE-2026-6687, CVE-2026-6688

First Published: April 17, 2026

Last Update: April 17, 2026

Status: Confirmed

Revision: 1.0

Executive Summary

In July 2026, security firm runZero disclosed a cluster of seven vulnerabilities affecting FatFs, a highly popular, lightweight open-source filesystem library. Because FatFs is the de facto standard used to read and write FAT/exFAT filesystems on microcontrollers, these bugs are deeply embedded in millions of consumer IoT devices, industrial controllers, drones, and medical hardware.

The primary risk stems from untrusted storage media (like an SD card or USB drive) or a malicious firmware update file. If a device mounts a specifically malformed filesystem image, the flaws are triggered. Because most bare-metal or real-time operating systems (RTOS) lack memory protections (like ASLR), successful exploitation can lead to a device "jailbreak" or permanent crash.

Overview:

****CVE-2026-6682****: CVSS 7.6 High

In FatFS R0.16 and earlier contains a FAT32 integer overflow bug in mount_volume() where fasize *= fs->n_fats can wrap, leading to attacker-controlled file-size metadata and unsafe read lengths in downstream callers. This maps to CWE-190 (Integer Overflow or Wraparound). Estimated CVSS v3.1 vector: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H (7.6, High).

Remote delivery is also possible in OTA/update pipelines. The estimated CISA SSVC vectors are Exploitation: PoC, Technical Impact: Total.

****CVE-2026-6683****: CVSS 4.6 Medium

FatFs R0.16 and earlier contains a divide-by-zero in exFAT sync logic bug when crafted metadata causes n_fatent - 2 to be zero during write/sync operations. This maps to CWE-369 (Divide By Zero). Estimated CVSS v3.1 vector: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H (4.6, Medium). Network-delivered update media can make this remote in some pipelines. The estimated CISA SSVC vectors are Exploitation: PoC, Technical Impact: Partial.

****CVE-2026-6684****: CVSS 4.6 Medium

FatFs prior to R0.16 that use GPT scanning with 'FF_LBA64 = 1' contains an issue where an unbounded loop count derived from GPT header field GPTH_PtNum, enabling extremely long or effectively infinite mount-time scans. This maps to CWE-835 (Loop with Unreachable Exit Condition). Estimated CVSS v3.1 vector: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H (4.6, Medium). The estimated CISA SSVC vectors are Exploitation: PoC, Technical Impact: Partial.

****CVE-2026-6685****: CVSS 6.1 Medium

FatFs R0.16 and earlier exhibits a stale dirty-cache skip via unsigned-subtraction wrap in f_read() / f_write() (fp->sect - sect < cc) during interleaved read/write on fragmented filesystems. This maps to CWE-191 (Integer Underflow). Estimated CVSS v3.1 vector: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H (6.1, Medium). The estimated CISA SSVC vectors are Exploitation: PoC, Technical Impact: Total.

****CVE-2026-6686****: CVSS 4.6 Medium

FatFs R0.16 and earlier contains an uninitialized cluster exposure when f_lseek() extends files beyond EOF without zero-filling newly allocated clusters. This maps to CWE-908 (Use of Uninitialized Resource). Estimated CVSS v3.1 vector: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N (4.6, Medium). The estimated CISA SSVC vectors are Exploitation: PoC, Technical Impact: Partial.

****CVE-2026-6687****: CVSS 7.6 High

FatFs R0.16 and earlier contains a stack overflow bug in f_getlabel() because exFAT label length (XDIR_NumLabel) is trusted without enforcing spec maximums. This maps to CWE-121 (Stack-based Buffer Overflow). Estimated CVSS v3.1 vector: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H (7.6, High). The estimated CISA SSVC vectors are Exploitation: PoC, Technical Impact: Total.

****CVE-2026-6688****: CVSS 7.6 High

FatFs R0.16 and earlier contains a downstream-caller vulnerability pattern associated with FatFs long filename handling. With LFN enabled, fno.fname can be up to 255 characters; many callers copy it into short fixed buffers without bounds checks, causing overflow. This maps to CWE-120 (Buffer Copy without Checking Size of Input). Estimated CVSS v3.1 vector: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H (7.6, High). The estimated CISA SSVC vectors are Exploitation: PoC, Technical Impact: Total.

Affected Products:

NONE

Workaround:

No Workaround Required

Solution:

No Solution Required

Revision History:

Revision	Date	Description
1.0	2026/7/15	Initial draft