ELAN Microelectronics Corp.
NO.12, INNOVATION RD.1, SCIENCE-BASED INDUSTRIAL PARK,
HSINCHU, TAIWAN, R.O.C.
Tel: +886-3-5639977

Vulnerability Report

Aug 6, 2026

Editorial Contact:
Tex Chen
ELAN Microelectronics Corp.
Tex_chen@emc.com.tw

CVE Identifier

CVE-2026-18909

Affected Projects

ELAN KMDF Driver Stack (ETD.sys / ETDSMBus.sys), applicable to systems using Intel SMBus interface.

Affected Versions

Versions prior to ETD24.21.52.3

Description

A stack buffer overflow vulnerability exists in the ELAN TouchPad driver stack on Intel SMBus platforms. ETDSMBus.sys does not enforce an upper-bound check on the hardware-derived report count received from the ELAN chip during Intel SMBus recovery. An out-of-range count value can be forwarded to ETD.sys, where it is used as the loop counter for a stack buffer copy operation without destination size validation, resulting in a stack buffer overflow and kernel bugcheck. The issue requires a third-party driver (CtiIo64.sys) as an SMBus access primitive to be exploitable by a local standard user. Either fix applied independently breaks the attack chain.

Vulnerability Type

Stack-based Buffer Overflow

CWE Classification

CWE-121: Stack-based Buffer Overflow

CVSS Scoring

CVSS v4.0 Base Score: 5.6 (Medium)
Vector:

CVSS:4.0/AV:L/AC:H/AT:P/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H/E:P/AU:N/R:U

CVSS v3.1 Base Score: 4.7 (Medium)
Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H

Impact
A local attacker can trigger a kernel bugcheck (BSOD: DRIVER_OVERRAN_STACK_BUFFER 0xF7) by exploiting unrestricted SMBus access through a vulnerable third-party driver to corrupt the ELAN SMBus communication state. The confirmed impact is Denial of Service. Kernel code execution has not been demonstrated.

Severity
Medium

Patch
Driver: ETD24.21.53.3

Acknowledgements
ELAN would like to thank the security researcher who responsibly reported this issue through our customer channel.