



Vulnerability Report

Jan 12, 2024

Editorial Contact:

Eric Lan
ELAN Microelectronics Corp.
eric.lan@emc.com.tw

CVE Identifier

CVE-2024-0454

Affected Projects

ELAN Match-on-Chip FPR Projects.

Affected Versions

Versions prior to 3.0.12011.08009 (Legacy) / 3.3.12011.08103 (ESS).

Description

Match-on-Chip FPR solution has design fault about risk of valid SID leakage and enumeration with spoof sensor. Windows Hello recognition would be bypass to cause broken account identity. Enhancement action is SDCP (Secure Device Connection Protocol) implementation to construct FPR sensor security validation procedures.

Vulnerability Type

Identity Security.

Impact

Issue would be encountered on Match-on-Chip FPR design without SDCP implementation (i.e. non-secure architecture).

Severity

Medium

Patch

Driver: 3.0.12011.08009 (Legacy) / 3.3.12011.08103 (ESS).

Acknowledgements

ELAN would like to thank BLACKWING INTELLIGENCE for reporting this issue.