Vulnerability Advisory

CVE ID	CVE-2024-37816
Title	Stack-based buffer overflow in EC25EUX
Description	The firmware within Quectel EC25EUXGAR08A05M1G is vulnerable to a stack-based buffer overflow when processing the AT+QIMSCFG command, which may lead to memory corruption and even service restart.
CWE	CWE-121 Stack-based Buffer Overflow
Score	4.2
Rating	Medium
CVSS String	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L
Affected Project	EC25-EUX
Affected Firmware	EC25EUXGAR08A05M1G
Assessment	Given that this vulnerability can only be triggered and exploited by trusted entities, the preconditions for exploitation are rather strict. Moreover, due to the memory protection mechanism, the vulnerability cannot be exploited in a targeted manner. Consequently, the actual impact of this vulnerability is quite limited.
Recommendation	Users of the affected products is recommended to upgrade the firmware to ensure the continued stability and security of the program's operation and to avoid any potential risks that might emerge in the future despite the current limited impact of the vulnerability.
Acknowledgement	Oliver Lavery and Harvey Phillips of Amazon Element55