# CVE Detail – CVE-2021-33478

The TrustZone implementation in certain Broadcom MediaxChange firmware could allow an unauthenticated, physically proximate attacker to achieve arbitrary code execution in the TrustZone Trusted Execution Environment (TEE) of an affected device. This, for example, affects certain Cisco IP Phone and Wireless IP Phone products before 2021-07-07. Exploitation is possible only when the attacker can disassemble the device in order to control the voltage/current for chip pins.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.33854

## CVSS Scoring

CVSS v3.1 Score: 6.8

Severity: MEDIUM

## Mapped CWE(s)

* CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

## CAPEC(s)

* CAPEC-10: Buffer Overflow via Environment Variables
* CAPEC-100: Overflow Buffers
* CAPEC-123: Buffer Manipulation
* CAPEC-14: Client-side Injection-induced Buffer Overflow
* CAPEC-24: Filter Failure through Buffer Overflow
* CAPEC-42: MIME Conversion
* CAPEC-44: Overflow Binary Resource File
* CAPEC-45: Buffer Overflow via Symbolic Links
* CAPEC-46: Overflow Variables and Tags
* CAPEC-47: Buffer Overflow via Parameter Expansion
* CAPEC-8: Buffer Overflow in an API Call
* CAPEC-9: Buffer Overflow in Local Command-Line Utilities

## Affected Products

* cpe:2.3:o:cisco:ip\_phone\_8800\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8800\_series\_with\_multiplatform\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8811\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8811\_with\_multiplatform\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8841\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8841\_with\_multiplatform\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8845\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8845\_with\_multiplatform\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8851\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8851\_with\_multiplatform\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8861\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8861\_with\_multiplatform\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8865\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8865\_with\_multiplatform\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:wireless\_ip\_phone\_8821\_firmware:\*:\*:\*:\*:\*:\*:\*:\*