# CVE Detail – CVE-2019-13945

A vulnerability has been identified in SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-1200 CPU family < V4.x (incl. SIPLUS variants) (All versions), SIMATIC S7-1200 CPU family V4.x (incl. SIPLUS variants) (All versions with Function State (FS) < 11), SIMATIC S7-200 SMART CPU CR20s (6ES7 288-1CR20-0AA1) (All versions <= V2.3.0 and Function State (FS) <= 3), SIMATIC S7-200 SMART CPU CR30s (6ES7 288-1CR30-0AA1) (All versions <= V2.3.0 and Function State (FS) <= 3), SIMATIC S7-200 SMART CPU CR40 (6ES7 288-1CR40-0AA0) (All versions <= V2.2.2 and Function State (FS) <= 8), SIMATIC S7-200 SMART CPU CR40s (6ES7 288-1CR40-0AA1) (All versions <= V2.3.0 and Function State (FS) <= 3), SIMATIC S7-200 SMART CPU CR60 (6ES7 288-1CR60-0AA0) (All versions <= V2.2.2 and Function State (FS) <= 10), SIMATIC S7-200 SMART CPU CR60s (6ES7 288-1CR60-0AA1) (All versions <= V2.3.0 and Function State (FS) <= 3), SIMATIC S7-200 SMART CPU SR20 (6ES7 288-1SR20-0AA0) (All versions <= V2.5.0 and Function State (FS) <= 11), SIMATIC S7-200 SMART CPU SR30 (6ES7 288-1SR30-0AA0) (All versions <= V2.5.0 and Function State (FS) <= 10), SIMATIC S7-200 SMART CPU SR40 (6ES7 288-1SR40-0AA0) (All versions <= V2.5.0 and Function State (FS) <= 10), SIMATIC S7-200 SMART CPU SR60 (6ES7 288-1SR60-0AA0) (All versions <= V2.5.0 and Function State (FS) <= 12), SIMATIC S7-200 SMART CPU ST20 (6ES7 288-1ST20-0AA0) (All versions <= V2.5.0 and Function State (FS) <= 9), SIMATIC S7-200 SMART CPU ST30 (6ES7 288-1ST30-0AA0) (All versions <= V2.5.0 and Function State (FS) <= 9), SIMATIC S7-200 SMART CPU ST40 (6ES7 288-1ST40-0AA0) (All versions <= V2.5.0 and Function State (FS) <= 8), SIMATIC S7-200 SMART CPU ST60 (6ES7 288-1ST60-0AA0) (All versions <= V2.5.0 and Function State (FS) <= 8), SIMATIC S7-200 SMART CPU family (All versions). There is an access mode used during manufacturing of the affected devices that allows additional diagnostic functionality. The security vulnerability could be exploited by an attacker with physical access to the UART interface during boot process.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.35611

## CVSS Scoring

CVSS v3.1 Score: 6.8

Severity: MEDIUM

## Mapped CWE(s)

* CWE-749: Exposed Dangerous Method or Function

## CAPEC(s)

* CAPEC-500: WebView Injection

## Affected Products

* cpe:2.3:o:siemens:simatic\_s7-1200\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:siemens:s7-200\_smart\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:siemens:simatic\_s7-200\_smart\_cpu\_st20\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:siemens:simatic\_s7-200\_smart\_cpu\_st30\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:siemens:simatic\_s7-200\_smart\_cpu\_st40\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:siemens:simatic\_s7-200\_smart\_cpu\_st60\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:siemens:simatic\_s7-200\_smart\_cpu\_sr20\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:siemens:simatic\_s7-200\_smart\_cpu\_sr30\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:siemens:simatic\_s7-200\_smart\_cpu\_sr40\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:siemens:simatic\_s7-200\_smart\_cpu\_sr60\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:siemens:simatic\_s7-200\_smart\_cpu\_cr40\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:siemens:simatic\_s7-200\_smart\_cpu\_cr60\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:siemens:simatic\_s7-200\_smart\_cpu\_cr20s\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:siemens:simatic\_s7-200\_smart\_cpu\_cr30s\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:siemens:simatic\_s7-200\_smart\_cpu\_cr40s\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:siemens:simatic\_s7-200\_smart\_cpu\_cr60s\_firmware:\*:\*:\*:\*:\*:\*:\*:\*