
1302 Peripherals, On-chip Fabric, and Interface/IO Problems
1191 Integration Issues
1190 Security Flow Issues
1329 Cross-Cutting Concerns
1189 Manufacturing and Life Cycle Management Concerns
1388 Power, Clock, Thermal, and Reset Concerns
1199 General Circuit and Logic Design Concerns
1366 Physical Access Issues and Concerns
1337 Debug and Test Problems
1350 Security Primitives and Cryptography Issues
1196 Privilege Separation and Access Control Issues
1431 Core and Compute Issues
1022 Memory and Storage Issues
1311 Improper Translation of Security Attributes by Fabric Bridge
1313 Missing Protection for Mirrored Regions in On-Chip Fabric Firewall
1315 Improper Setting of Bus Controlling Capability in Fabric Endpoint
1316 Fabric-Address Map Allows Programming of Unintended Overlaps of Protected and Unprotected Ranges
1317 Improper Access Control in Fabric Bridge
1331 Improper Isolation of Shared Resources in Network On Chip (NoC)
1276 Improper Request Propagation before Data Reception in Write Transactions in a Bus Architecture
1276 Hardware Child Block Incorrectly Connected to Parent System
1196 Shared Device Enabled Too Early in Boot Phase
1193 Power-On of Untrusted Execution Core Before Enabling Fabric Access Control
1363 Hardware Logic with Insecure De-Synchronization between Control and Data Channels
1274 Improper Access Control for Volatile Memory Containing Boot Code
1389 Mutable Attestation or Measurement Reporting Data
1413 Missing Ability to Patch ROM Code
1326 Missing Immutable Root of Trust in Hardware
1328 Security Version Number Mutable in Older Versions
1053 Missing Documentation for Design
1052 Improper Physical Access Control
1277 Firmware Not Updateable
1281 Insufficient or Incomplete Data Removal within Hardware Component
1329 Reliance on Component That is Not Updateable
1280 Persistent Data Readable after Memory Erase
1247 Reliance on Insufficiently Trustworthy Component
1429 Missing Security-Relevant Feedback for Unexecuted Operations in Hardware Interface
1357 Reliance on Insufficiently Trustworthy Component
1053 Insufficient Technical Documentation
1417 Hardware Simulation / Synthesis Mismatch
1384 Improper Scrubbing of Sensitive Data from Decommissioned Device
1309 Product Released in Non-Release Configuration
1073 Device Unique Credential Sharing
1367 Unprotected Confidential Information on Device is Accessible by OSAT Vendor
1323 Improper Protections Against Hardware Overheating
1308 Semiconductor Defects in Hardware Logic with Security-Sensitive Implications
1196 Improper Restriction of Software Interfaces to Hardware Features
1384 Improperly Preserved Integrity of Hardware Configuration State During a Power Glitch/Reduced Operation
1255 Improper Protection for Outbound Error Messages and Alert Signals
1271 Uninitialized Value on Reset for Registers Holding Security Settings
1332 Improper Lock Behavior After Power-State Transition
1247 Improper Protection Against Voltage and Clock Glitches
1254 Incorrect Comparison Logic Granularity
1328 Security-Sensitive Hardware Controls with Missing Lock Bit Protection
1245 Improper Finite State Machines (FSMs) in Hardware Logic
1280 Improper Preservation of Consistency Between Independent Representations of Shared State
1253 Incorrect Selection of Fuse Values
1254 Incorrect Comparison Logic Granularity
1298 Hardware Logic Contains Race Conditions
1367 Improper Handling of Single Event Upsets
1234 Hardware Internal or Debug Modes Allow Override of Locks
1274 Improper Protection against Electromagnetic Fault Injection (EM FI)
1384 Improper Handling of Physical or Environmental Conditions
1278 Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques
1247 Improper Handling of Hardware Behavior in Exceptionally Cold Environments
1243 Sensitive Non-Volatile Information Not Protected During Debug
1191 On-Chip Debug and Test Interface With Improper Access Control
1313 Missing Write Protection for Parametric Data Values
1244 Internal Asset Exposed to Unsafe Debug Access Level or State
1459 Exposure of Sensitive System Information Due to Uncleared Debug Information
1384 Improper Protection of Physical Side Channels
1272 Sensitive Information Uncleared Before Debug/Power State Transition
1391 Use of Weak Credentials
1191 On-Chip Debug and Test Interface With Improper Access Control
1256 Improper Restriction of Power Consumption Profile
1313 Missing Write Protection for Parametric Data Values
1244 Internal Asset Exposed to Unsafe Debug Access Level or State
1459 Exposure of Sensitive System Information Due to Uncleared Debug Information
1384 Improper Protection of Physical Side Channels
1272 Sensitive Information Uncleared Before Debug/Power State Transition
1391 Use of Weak Credentials
1245 Improper Finite State Machines (FSMs) in Hardware Logic
1256 Improper Restriction of Power Consumption Profile
1303 Non-Transparent Sharing of Microarchitectural Resources
1191 On-Chip Debug and Test Interface With Improper Access Control
1300 Improper Protection of Physical Side Channels
1240 Use of a Cryptographic Primitive with a Risky Implementation
1241 Use of Predictable Algorithm in Random Number Generator
1279 Cryptographic Operations are Run Before Supporting Units are Ready
1431 Driving Intermediate Cryptographic State/Results to Hardware Blocks/Outputs
1282 Assumed-Immutable Data is Stored in Writable Memory
1254 Incorrect Comparison Logic Granularity
1276 Hardware Child Block Incorrectly Connected to Parent System
1191 On-Chip Debug and Test Interface With Improper Access Control
1421 Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution
1420 Exposure of Sensitive Information during Transient Execution
1303 Non-Transparent Sharing of Microarchitectural Resources
1420 Exposure of Sensitive Information caused by Incorrect Data Forwarding during Transient Execution
1421 Exposure of Sensitive Information caused by Shared Microarchitectural Predictor State that Influences Transient Execution
1342 Information Exposure through Microarchitectural State after Transient Execution
1189 Improper Isolation of Shared Resources on System-on-a-Chip (SoC)
1190 Improper Identifier for IP Block used in System-On-Chip (SOC)
1420 Exposure of Sensitive Information during Transient Execution
1421 Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution
1420 Exposure of Sensitive Information caused by Incorrect Data Forwarding during Transient Execution
1421 Exposure of Sensitive Information caused by Shared Microarchitectural Predictor State that Influences Transient Execution
1342 Information Exposure through Microarchitectural State after Transient Execution