TERRIER CVE ANALYSIS MINI REPORT

Embedded Systems Edition 1/9/2024

QVLX LLC

600 BOULEVARD SOUTH SOUTHWEST SUITE 104, HUNTSVILLE, AL, USA
SEE COMPANION DASHBOARD: RESEARCH - QVLX LABS

NOTICE

THE RAW DATA THAT WENT INTO THIS REPORT SOURCED FROM THE MITRE CVE DATABASE. ALL CREDIT AND RESPONSIBILITY REGARDING THAT DATA BELONGS TO MITRE CORPORATION.

THE ANALYSIS PERFORMED ON THE DATA IS A PROPRIETARY COCKTAIL PROVIDED BY QVLX LLC'S TERRIER ANALYSIS PLATFORM WHICH INCLUDES A BLEND OF IN-HOUSE MACHINE LEARNING (ENSEMBLE) ALGORITHMS, OPENAI CHATGPT4, AND GOOGLE BARD ANALYSIS. ALL CREDIT PERTAINING TO USE OF CHATGPT AND BARD BELONG TO THEIR RESPECTIVE OWNERS. IN THE NAME OF ACADEMIC PROGRESS, HUMBLY THANK YOU ALL FOR THE TOOLS TO THRIVE.

KEYWORD SEARCHES YIELDING NO ENTRIES AT ALL WERE OMITTED DURING PREPROCESSING.

TERRIER CVE ANALYSIS MINI REPORT (EMBEDDED/IOT FOCUS)

MULTI-DIMENSIONAL AI-BASED STUDY

TABLE OF CONTENTS

CVE DATA ANALYSIS REPORT: EMBEDDED SYSTEMS (2018-2023)

Executive Summary:

- The analysis focuses on hardware component-related CVEs over the years 2018 to 2023.
- BLE (Bluetooth Low Energy) and RAM show the highest percentage of CVEs.
- Certain components like Thunderbolt Interface, WLAN Adapter, and various others consistently report zero CVEs.
- IoT and Embedded Systems display a notable presence in CVEs, particularly in BLE-related vulnerabilities.

Data Exclusion Note: The following components reported zero CVEs and are therefore excluded from detailed analysis: Southbridge, Northbridge, SATA, DisplayPort, FPGA, Cortex-M, Cortex-A, Security Processing Unit, Platform Security Architecture, Confidential Computing Architecture.

Data Overview:

- **Total CVEs Analyzed:** 140,184 over five years.
- **High Vulnerability Components:** BLE, ROM, RAM, WLAN, USB, GPU, ASIC.
- **Low/Zero Occurrence Components:** Serial Peripheral Interface, Serial Communication Interface, Thunderbolt, Smart Card Reader.

**Notable increases in USB, GPU, WLAN, and ASIC vulnerabilities over time, indicating evolving security risks.

Yearly Breakdown:

- **2018:** BLE (39.48%) and ROM (13.74%) led in vulnerabilities. Emerging concerns in WLAN and ASIC indicated broadening attack surfaces.
- **2019:** BLE (42.39%) saw an increase, while vulnerabilities in USB and WLAN showed significant growth.
- **2020:** BLE (52.17%) continued to dominate. Noticeable increases in GPU and WLAN vulnerabilities highlighted growing security concerns.
- **2021:** BLE (49.71%) remained high, while vulnerabilities in GPU and WLAN continued to rise, emphasizing the need for secure communication protocols.

- **2022:** BLE (49.52%) and WLAN (0.52%) vulnerabilities underscored the critical importance of wireless communication security. ASIC vulnerabilities also rose, reflecting the expanding role of specialized hardware.
- **2023:** BLE (62.00%) reached its peak, and WLAN vulnerabilities continued to grow, emphasizing the need for robust wireless security measures.

Yearly Implications:

- **2018-2019:** Initial years showed a dominance of vulnerabilities in BLE and ROM. Emergence of issues in WLAN and ASIC components.
- **2020-2021:** A spike in BLE vulnerabilities, coupled with rising threats in GPU and WLAN, suggested increasing risks in wireless and graphic processing units.
- **2022-2023:** BLE vulnerabilities peaked, with WLAN also showing substantial increase. This period marked a heightened risk in wireless communication systems.

Analysis of IoT and Embedded Systems: Given the high prevalence of vulnerabilities in BLE, WLAN, and other communication-related components, there is an urgent need for enhanced security protocols in IoT and embedded systems. The consistent vulnerabilities in memory components (ROM, RAM) highlight the importance of secure memory management.

Zero Occurrence Areas: Some components such as Serial Peripheral Interface, Serial Communication Interface, Thunderbolt, and Smart Card Reader showed zero occurrences in CVEs, indicating either lower risk or underreporting in these areas.

Strategic Recommendations:

1. **Focus on BLE Security:** Allocate significant resources to investigate and mitigate vulnerabilities in BLE technology, crucial for IoT device security.
2. **RAM and ROM Security Enhancements:** Develop robust security protocols for memory components, addressing both physical and software-based attacks.
3. **Processor Security Research:** Intensify research on CPU vulnerabilities, particularly in the context of multi-core and advanced processing units.
4. **IoT Device Security:** Emphasize the development of secure firmware and hardware-level protections for IoT devices, given the high rate of BLE and other related component vulnerabilities.
5. **Regular Hardware Security Audits:** Conduct regular security audits of hardware components, including ADC, DAC, and various communication interfaces, to identify and address vulnerabilities proactively.

6. **Community Engagement and Awareness:** Promote awareness about hardware component vulnerabilities among manufacturers and developers, encouraging the adoption of secure design practices.
7. **Enhanced Monitoring and Incident Response:** Develop advanced monitoring systems to detect anomalies in hardware behavior and establish rapid incident response mechanisms for hardware-related security breaches.

CONCLUSION

The analysis of CVE data from 2018 to 2023 reveals a dynamic and evolving landscape of vulnerabilities in hardware components, with a particularly sharp focus on BLE, RAM, and CPUs. The significant prevalence of vulnerabilities in these areas underscores the necessity for ongoing vigilance, enhanced security protocols, and proactive measures in both IoT and traditional computing environments. As technology continues to advance, it becomes imperative for cybersecurity efforts to adapt and address these challenges, ensuring robust protection against potential hardware-related threats. This continuous evolution in hardware security is not just a technological challenge but a critical aspect of maintaining trust and integrity in the digital infrastructure that underpins modern society.

DIMENSIONS ANALYZED AND CLUSTERING

Dimension	Cluster
Cache	IoT
CPU	
Ethernet	
PCI	
IC	
SPI	
Serial Peripheral Interface	
Serial Communication Interface	
Serial Port	
CANbus	
Modbus	
SCSI	
VMM	
UEFI	
TrustZone	
Flash Memory	
ROM	
RAM	
CD-ROM	
USB	
Bluetooth	
BLE	

Dimension	Cluster
IOMMU	
SATA	
NVMe	
GPU	
DSP	
FPGA	
ASIC	
Thunderbolt Interface	
HDMI	
VGA	
DisplayPort	
WLAN Adapter	
RFID Reader	
NFC Interface	
Smart Card Reader	
BIOS	
CMOS	
Southbridge	
Northbridge	
TPM	
VRM	
PLL	
M Connector	
PS/ Port	
Audio Codec Chip	
ADC	
DAC	
Temperature Sensors	
Fan Controllers	
BSP	
VME	
VPX	
cPCI	
zigbee	
mqtt	
uart	
jtag	
firmware	
u-boot	
microkernel	
MCU	
MPU	
MMU	
disk	
SSD	
nvme	

Dimension	Cluster
spacewire	
smbus	
SDIO	
MDIO	
ACPI	
microcode	
SGX	
Intel Management Engine	
Trusted Platform Module	
Intel Platform Trust Technology	
PTT	
Intel Software Guard Extensions	
Intel Trusted Execution Technology	
TXT	
Intel Speed Shift Technology	
Intel Turbo Boost Technology	
Intel Quick Sync Video	
Intel Optane Memory	
Cortex-M	
Cortex-A	
Security Processing Unit	
SPU	
Platform Security Architecture	
PSA	
CryptoCell	
Confidential Computing Architecture	
CCA	

RAW RESULTS

Filter Year: ALL
Total CVEs: 290756
Cache: 0.53% (1527)
CPU: 0.59% (1723)
Ethernet: 0.16% (468)
PCI: 0.06% (175)
I2C: 0.01% (25)
SPI: 0.33% (960)
Serial Peripheral Interface: 0.00% (4)
Serial Communication Interface: 0.00% (0)
Serial Port: 0.01% (29)
CANbus: 0.00% (1)
Modbus: 0.04% (128)
SCSI: 0.07% (193)
VMM: 0.01% (37)
UEFI: 0.04% (115)
TrustZone: 0.05% (150)
Flash Memory: 0.01% (34)
ROM: 10.78% (31345)
RAM: 12.02% (34955)

CD-ROM: 0.00% (11)
USB: 0.25% (714)
Bluetooth: 0.26% (749)
BLE: 37.76% (109799)
IOMMU: 0.02% (50)
SATA: 0.01% (22)
NVMe: 0.01% (27)
GPU: 0.20% (572)
DSP: 0.07% (191)
FPGA: 0.01% (21)
ASIC: 0.25% (741)
Thunderbolt: 0.01% (31)
HDMI: 0.01% (16)
VGA: 0.03% (85)
DisplayPort: 0.00% (0)
WLAN: 0.18% (536)
RFID: 0.01% (17)
NFC: 0.06% (176)
Smartcard: 0.01% (26)
BIOS: 0.17% (502)
CMOS: 0.00% (5)
Southbridge: 0.00% (1)
Northbridge: 0.00% (0)
TPM: 0.03% (82)
VRM: 0.03% (92)
PLL: 0.00% (4)
M.2: 0.00% (2)
PS/2 Port: 0.00% (0)
Audio Codec Chip: 0.00% (0)
ADC: 0.27% (780)
DAC: 0.09% (267)
Thermocouple: 0.00% (0)
Fan Controller: 0.00% (0)
BSP: 0.32% (936)
VME: 0.02% (51)
VPX: 0.01% (33)
cPCI: 0.00% (7)
zigbee: 0.01% (27)
mqtt: 0.04% (126)
uart: 0.06% (171)
jtag: 0.00% (5)
firmware: 1.45% (4228)
u-boot: 0.02% (45)
microkernel: 0.04% (104)
MCU: 0.01% (41)
MPU: 0.75% (2187)
MMU: 1.05% (3044)
disk: 0.31% (909)
SSD: 0.09% (267)
nvme: 0.01% (27)
1553: 0.01% (20)
spacewire: 0.00% (0)
smbus: 0.00% (5)
SDIO: 0.00% (2)
MDIO: 0.00% (2)
ACPI: 0.02% (53)
microcode: 0.01% (20)
SGX: 0.03% (82)
Intel Management Engine: 0.00% (1)
Trusted Platform Module: 0.00% (13)
Intel Platform Trust Technology: 0.00% (0)
PTT: 0.01% (22)
Intel Software Guard Extensions: 0.00% (3)
Intel Trusted Execution Technology: 0.00% (2)
TXT: 0.18% (510)
Intel Speed Shift Technology: 0.00% (0)
Intel Turbo Boost Technology: 0.00% (0)
Intel Quick Sync Video: 0.00% (0)
Intel Optane Memory: 0.00% (1)
Cortex-M: 0.00% (2)
Cortex-A: 0.00% (2)
Security Processing Unit: 0.00% (0)
SPU: 0.44% (1290)
Platform Security Architecture: 0.00% (0)
PSA: 0.03% (74)

```
CryptoCell: 0.00% (2)
Confidential Computing Architecture: 0.00% (0)
CCA: 0.04% (103)

Filter Year: 2018
Total CVEs: 21922
Cache: 0.52% (115)
CPU: 0.30% (66)
Ethernet: 0.15% (32)
PCI: 0.05% (11)
I2C: 0.00% (1)
SPI: 0.38% (84)
Serial Peripheral Interface: 0.00% (0)
Serial Communication Interface: 0.00% (0)
Serial Port: 0.01% (2)
CANbus: 0.00% (0)
Modbus: 0.13% (28)
SCSI: 0.05% (10)
VMM: 0.01% (2)
UEFI: 0.03% (7)
TrustZone: 0.03% (6)
Flash Memory: 0.02% (4)
ROM: 13.74% (3011)
RAM: 8.53% (1871)
CD-ROM: 0.00% (0)
USB: 0.14% (31)
Bluetooth: 0.21% (47)
BLE: 39.48% (8654)
IOMMU: 0.01% (2)
SATA: 0.00% (0)
NVMe: 0.01% (2)
GPU: 0.07% (16)
DSP: 0.09% (20)
FPGA: 0.00% (0)
ASIC: 0.21% (45)
Thunderbolt: 0.00% (0)
HDMI: 0.00% (1)
VGA: 0.03% (7)
DisplayPort: 0.00% (0)
WLAN: 0.34% (75)
RFID: 0.01% (3)
NFC: 0.05% (11)
Smartcard: 0.07% (16)
BIOS: 0.04% (9)
CMOS: 0.00% (0)
Southbridge: 0.00% (0)
Northbridge: 0.00% (0)
TPM: 0.01% (3)
VRM: 0.05% (12)
PLL: 0.00% (0)
M.2: 0.00% (0)
PS/2 Port: 0.00% (0)
Audio Codec Chip: 0.00% (0)
ADC: 0.28% (61)
DAC: 0.09% (19)
Thermocouple: 0.00% (0)
Fan Controller: 0.00% (0)
BSP: 0.27% (59)
VME: 0.02% (4)
VPX: 0.00% (1)
cPCI: 0.00% (0)
zigbee: 0.01% (2)
mqtt: 0.05% (11)
uart: 0.06% (13)
jtag: 0.00% (1)
firmware: 1.97% (431)
u-boot: 0.02% (5)
microkernel: 0.02% (4)
MCU: 0.01% (2)
MPU: 0.80% (176)
MMU: 1.19% (261)
disk: 0.57% (124)
SSD: 0.08% (18)
nvme: 0.01% (2)
1553: 0.01% (3)
```

```
spacewire: 0.00% (0)
smbus: 0.01% (2)
SDIO: 0.00% (0)
MDIO: 0.00% (1)
ACPI: 0.01% (2)
microcode: 0.01% (3)
SGX: 0.04% (8)
Intel Management Engine: 0.00% (0)
Trusted Platform Module: 0.00% (1)
Intel Platform Trust Technology: 0.00% (0)
PTT: 0.01% (2)
Intel Software Guard Extensions: 0.01% (2)
Intel Trusted Execution Technology: 0.00% (0)
TXT: 0.11% (25)
Intel Speed Shift Technology: 0.00% (0)
Intel Turbo Boost Technology: 0.00% (0)
Intel Quick Sync Video: 0.00% (0)
Intel Optane Memory: 0.00% (1)
Cortex-M: 0.00% (0)
Cortex-A: 0.00% (0)
Security Processing Unit: 0.00% (0)
SPU: 0.69% (152)
Platform Security Architecture: 0.00% (0)
PSA: 0.04% (8)
CryptoCell: 0.00% (0)
Confidential Computing Architecture: 0.00% (0)
CCA: 0.05% (10)

Filter Year: 2019
Total CVEs: 21560
Cache: 0.61% (131)
CPU: 0.40% (87)
Ethernet: 0.28% (61)
PCI: 0.11% (23)
I2C: 0.01% (2)
SPI: 0.32% (69)
Serial Peripheral Interface: 0.00% (0)
Serial Communication Interface: 0.00% (0)
Serial Port: 0.01% (3)
CANbus: 0.00% (0)
Modbus: 0.10% (22)
SCSI: 0.05% (11)
VMM: 0.00% (1)
UEFI: 0.02% (5)
TrustZone: 0.03% (6)
Flash Memory: 0.01% (2)
ROM: 13.14% (2834)
RAM: 5.77% (1243)
CD-ROM: 0.00% (0)
USB: 0.44% (95)
Bluetooth: 0.53% (115)
BLE: 42.39% (9139)
IOMMU: 0.02% (4)
SATA: 0.00% (0)
NVMe: 0.00% (0)
GPU: 0.21% (46)
DSP: 0.06% (12)
FPGA: 0.03% (7)
ASIC: 0.26% (55)
Thunderbolt: 0.01% (2)
HDMI: 0.00% (0)
VGA: 0.01% (3)
DisplayPort: 0.00% (0)
WLAN: 0.23% (49)
RFID: 0.02% (4)
NFC: 0.14% (31)
Smartcard: 0.00% (0)
BIOS: 0.08% (17)
CMOS: 0.00% (1)
Southbridge: 0.00% (0)
Northbridge: 0.00% (0)
TPM: 0.02% (4)
VRM: 0.04% (8)
PLL: 0.00% (0)
M.2: 0.00% (1)
```

```
PS/2 Port: 0.00% (0)
Audio Codec Chip: 0.00% (0)
ADC: 0.22% (47)
DAC: 0.09% (20)
Thermocouple: 0.00% (0)
Fan Controller: 0.00% (0)
BSP: 0.17% (36)
VME: 0.01% (2)
VPX: 0.02% (4)
cPCI: 0.00% (0)
zigbee: 0.04% (8)
mqtt: 0.08% (17)
uart: 0.06% (13)
jtag: 0.00% (1)
firmware: 2.22% (478)
u-boot: 0.09% (20)
microkernel: 0.02% (4)
MCU: 0.02% (4)
MPU: 1.74% (376)
MMU: 1.68% (363)
disk: 0.24% (51)
SSD: 0.09% (19)
nvme: 0.00% (0)
1553: 0.00% (1)
spacewire: 0.00% (0)
smbus: 0.00% (0)
SDIO: 0.00% (1)
MDIO: 0.00% (1)
ACPI: 0.00% (1)
microcode: 0.00% (1)
SGX: 0.06% (14)
Intel Management Engine: 0.00% (0)
Trusted Platform Module: 0.00% (1)
Intel Platform Trust Technology: 0.00% (0)
PTT: 0.01% (2)
Intel Software Guard Extensions: 0.00% (0)
Intel Trusted Execution Technology: 0.00% (0)
TXT: 0.11% (24)
Intel Speed Shift Technology: 0.00% (0)
Intel Turbo Boost Technology: 0.00% (0)
Intel Quick Sync Video: 0.00% (0)
Intel Optane Memory: 0.00% (0)
Cortex-M: 0.00% (1)
Cortex-A: 0.00% (1)
Security Processing Unit: 0.00% (0)
SPU: 0.59% (128)
Platform Security Architecture: 0.00% (0)
PSA: 0.01% (2)
CryptoCell: 0.00% (0)
Confidential Computing Architecture: 0.00% (0)
CCA: 0.05% (11)

Filter Year: 2020
Total CVEs: 31337
Cache: 0.41% (127)
CPU: 0.28% (88)
Ethernet: 0.21% (67)
PCI: 0.05% (15)
I2C: 0.00% (0)
SPI: 0.27% (85)
Serial Peripheral Interface: 0.00% (0)
Serial Communication Interface: 0.00% (0)
Serial Port: 0.00% (1)
CANbus: 0.00% (0)
Modbus: 0.04% (11)
SCSI: 0.04% (14)
VMM: 0.02% (5)
UEFI: 0.03% (9)
TrustZone: 0.08% (24)
Flash Memory: 0.02% (7)
ROM: 11.94% (3742)
RAM: 6.34% (1988)
CD-ROM: 0.00% (0)
USB: 0.23% (71)
Bluetooth: 0.32% (101)
```

```
BLE: 52.17% (16350)
IOMMU: 0.01% (3)
SATA: 0.01% (2)
NVMe: 0.01% (3)
GPU: 0.14% (43)
DSP: 0.04% (13)
FPGA: 0.02% (5)
ASIC: 0.17% (53)
Thunderbolt: 0.05% (15)
HDMI: 0.00% (0)
VGA: 0.04% (14)
DisplayPort: 0.00% (0)
WLAN: 0.07% (22)
RFID: 0.00% (1)
NFC: 0.14% (44)
Smartcard: 0.00% (0)
BIOS: 0.16% (51)
CMOS: 0.00% (0)
Southbridge: 0.00% (0)
Northbridge: 0.00% (0)
TPM: 0.02% (7)
VRM: 0.00% (0)
PLL: 0.00% (0)
M.2: 0.00% (0)
PS/2 Port: 0.00% (0)
Audio Codec Chip: 0.00% (0)
ADC: 0.23% (72)
DAC: 0.07% (21)
Thermocouple: 0.00% (0)
Fan Controller: 0.00% (0)
BSP: 0.12% (38)
VME: 0.02% (5)
VPX: 0.00% (0)
cPCI: 0.00% (0)
zigbee: 0.02% (5)
mqtt: 0.04% (11)
uart: 0.05% (15)
jtag: 0.00% (0)
firmware: 1.41% (442)
u-boot: 0.01% (3)
microkernel: 0.06% (20)
MCU: 0.00% (0)
MPU: 1.19% (374)
MMU: 1.01% (318)
disk: 0.18% (56)
SSD: 0.10% (31)
nvme: 0.01% (3)
1553: 0.00% (1)
spacewire: 0.00% (0)
smbus: 0.00% (0)
SDIO: 0.00% (0)
MDIO: 0.00% (0)
ACPI: 0.01% (4)
microcode: 0.01% (2)
SGX: 0.04% (14)
Intel Management Engine: 0.00% (0)
Trusted Platform Module: 0.01% (4)
Intel Platform Trust Technology: 0.00% (0)
PTT: 0.00% (1)
Intel Software Guard Extensions: 0.00% (0)
Intel Trusted Execution Technology: 0.00% (0)
TXT: 0.08% (24)
Intel Speed Shift Technology: 0.00% (0)
Intel Turbo Boost Technology: 0.00% (0)
Intel Quick Sync Video: 0.00% (0)
Intel Optane Memory: 0.00% (0)
Cortex-M: 0.00% (0)
Cortex-A: 0.00% (0)
Security Processing Unit: 0.00% (0)
SPU: 0.33% (102)
Platform Security Architecture: 0.00% (0)
PSA: 0.01% (3)
CryptoCell: 0.00% (0)
Confidential Computing Architecture: 0.00% (0)
CCA: 0.03% (9)
```

```
Filter Year: 2021
Total CVEs: 30717
Cache: 0.42% (128)
CPU: 0.42% (130)
Ethernet: 0.24% (75)
PCI: 0.06% (18)
I2C: 0.00% (0)
SPI: 0.27% (82)
Serial Peripheral Interface: 0.00% (0)
Serial Communication Interface: 0.00% (0)
Serial Port: 0.02% (5)
CANbus: 0.00% (0)
Modbus: 0.05% (16)
SCSI: 0.05% (14)
VMM: 0.00% (1)
UEFI: 0.07% (21)
TrustZone: 0.07% (22)
Flash Memory: 0.01% (4)
ROM: 12.07% (3709)
RAM: 8.26% (2537)
CD-ROM: 0.00% (1)
USB: 0.27% (83)
Bluetooth: 0.34% (104)
BLE: 49.71% (15268)
IOMMU: 0.03% (10)
SATA: 0.00% (0)
NVMe: 0.03% (8)
GPU: 0.28% (86)
DSP: 0.07% (21)
FPGA: 0.00% (0)
ASIC: 0.18% (56)
Thunderbolt: 0.00% (1)
HDMI: 0.01% (3)
VGA: 0.01% (2)
DisplayPort: 0.00% (0)
WLAN: 0.10% (31)
RFID: 0.01% (3)
NFC: 0.08% (26)
Smartcard: 0.01% (2)
BIOS: 0.22% (68)
CMOS: 0.00% (0)
Southbridge: 0.00% (0)
Northbridge: 0.00% (0)
TPM: 0.03% (9)
VRM: 0.07% (22)
PLL: 0.00% (0)
M.2: 0.00% (0)
PS/2 Port: 0.00% (0)
Audio Codec Chip: 0.00% (0)
ADC: 0.26% (79)
DAC: 0.08% (26)
Thermocouple: 0.00% (0)
Fan Controller: 0.00% (0)
BSP: 0.08% (26)
VME: 0.04% (12)
VPX: 0.00% (1)
cPCI: 0.00% (1)
zigbee: 0.00% (0)
mqtt: 0.08% (26)
uart: 0.03% (9)
jtag: 0.00% (0)
firmware: 1.69% (519)
u-boot: 0.01% (2)
microkernel: 0.06% (17)
MCU: 0.03% (9)
MPU: 1.00% (307)
MMU: 1.00% (308)
disk: 0.32% (98)
SSD: 0.10% (31)
nvme: 0.03% (8)
1553: 0.04% (11)
spacewire: 0.00% (0)
smbus: 0.00% (0)
SDIO: 0.00% (0)
```

```
MDIO: 0.00% (0)
ACPI: 0.01% (4)
microcode: 0.02% (5)
SGX: 0.07% (20)
Intel Management Engine: 0.00% (0)
Trusted Platform Module: 0.00% (0)
Intel Platform Trust Technology: 0.00% (0)
PTT: 0.02% (7)
Intel Software Guard Extensions: 0.00% (0)
Intel Trusted Execution Technology: 0.00% (0)
TXT: 0.09% (28)
Intel Speed Shift Technology: 0.00% (0)
Intel Turbo Boost Technology: 0.00% (0)
Intel Quick Sync Video: 0.00% (0)
Intel Optane Memory: 0.00% (0)
Cortex-M: 0.00% (1)
Cortex-A: 0.00% (0)
Security Processing Unit: 0.00% (0)
SPU: 0.26% (79)
Platform Security Architecture: 0.00% (0)
PSA: 0.05% (16)
CryptoCell: 0.00% (1)
Confidential Computing Architecture: 0.00% (0)
CCA: 0.03% (10)

Filter Year: 2022
Total CVEs: 33470
Cache: 0.38% (128)
CPU: 0.29% (96)
Ethernet: 0.15% (49)
PCI: 0.04% (12)
I2C: 0.02% (8)
SPI: 0.41% (136)
Serial Peripheral Interface: 0.00% (0)
Serial Communication Interface: 0.00% (0)
Serial Port: 0.02% (7)
CANbus: 0.00% (0)
Modbus: 0.04% (14)
SCSI: 0.05% (17)
VMM: 0.01% (2)
UEFI: 0.05% (17)
TrustZone: 0.00% (0)
Flash Memory: 0.02% (6)
ROM: 9.33% (3122)
RAM: 9.08% (3038)
CD-ROM: 0.01% (3)
USB: 0.28% (93)
Bluetooth: 0.38% (127)
BLE: 49.52% (16576)
IOMMU: 0.05% (17)
SATA: 0.01% (4)
NVMe: 0.02% (7)
GPU: 0.32% (108)
DSP: 0.06% (20)
FPGA: 0.01% (5)
ASIC: 0.32% (106)
Thunderbolt: 0.00% (0)
HDMI: 0.01% (4)
VGA: 0.01% (2)
DisplayPort: 0.00% (0)
WLAN: 0.52% (173)
RFID: 0.00% (1)
NFC: 0.08% (27)
Smartcard: 0.00% (0)
BIOS: 0.54% (180)
CMOS: 0.00% (0)
Southbridge: 0.00% (0)
Northbridge: 0.00% (0)
TPM: 0.04% (14)
VRM: 0.04% (14)
PLL: 0.00% (0)
M.2: 0.00% (1)
PS/2 Port: 0.00% (0)
Audio Codec Chip: 0.00% (0)
ADC: 0.28% (94)
```

```
DAC: 0.11% (36)
Thermocouple: 0.00% (0)
Fan Controller: 0.00% (0)
BSP: 0.07% (24)
VME: 0.02% (8)
VPX: 0.00% (0)
cPCI: 0.00% (0)
zigbee: 0.01% (2)
mqtt: 0.05% (16)
uart: 0.25% (85)
jtag: 0.01% (2)
firmware: 1.34% (449)
u-boot: 0.03% (10)
microkernel: 0.08% (28)
MCU: 0.01% (5)
MPU: 0.56% (187)
MMU: 1.24% (414)
disk: 0.25% (83)
SSD: 0.09% (29)
nvme: 0.02% (7)
1553: 0.00% (0)
spacewire: 0.00% (0)
smbus: 0.01% (2)
SDIO: 0.00% (0)
MDIO: 0.00% (0)
ACPI: 0.04% (13)
microcode: 0.01% (2)
SGX: 0.04% (12)
Intel Management Engine: 0.00% (0)
Trusted Platform Module: 0.00% (1)
Intel Platform Trust Technology: 0.00% (0)
PTT: 0.01% (2)
Intel Software Guard Extensions: 0.00% (0)
Intel Trusted Execution Technology: 0.00% (0)
TXT: 0.14% (47)
Intel Speed Shift Technology: 0.00% (0)
Intel Turbo Boost Technology: 0.00% (0)
Intel Quick Sync Video: 0.00% (0)
Intel Optane Memory: 0.00% (0)
Cortex-M: 0.00% (0)
Cortex-A: 0.00% (0)
Security Processing Unit: 0.00% (0)
SPU: 0.24% (79)
Platform Security Architecture: 0.00% (0)
PSA: 0.01% (4)
CryptoCell: 0.00% (0)
Confidential Computing Architecture: 0.00% (0)
CCA: 0.04% (12)

Filter Year: 2023
Total CVEs: 32975
Cache: 0.36% (119)
CPU: 0.18% (60)
Ethernet: 0.09% (30)
PCI: 0.04% (12)
I2C: 0.01% (4)
SPI: 0.28% (91)
Serial Peripheral Interface: 0.00% (1)
Serial Communication Interface: 0.00% (0)
Serial Port: 0.00% (1)
CANbus: 0.00% (0)
Modbus: 0.02% (7)
SCSI: 0.04% (14)
VMM: 0.01% (2)
UEFI: 0.11% (37)
TrustZone: 0.01% (2)
Flash Memory: 0.01% (3)
ROM: 6.73% (2219)
RAM: 6.82% (2250)
CD-ROM: 0.00% (0)
USB: 0.15% (48)
Bluetooth: 0.24% (78)
BLE: 62.00% (20446)
IOMMU: 0.01% (4)
SATA: 0.00% (0)
```

NVMe: 0.02% (5)
GPU: 0.13% (43)
DSP: 0.04% (12)
FPGA: 0.01% (2)
ASIC: 0.22% (72)
Thunderbolt: 0.00% (1)
HDMI: 0.00% (0)
VGA: 0.00% (0)
DisplayPort: 0.00% (0)
WLAN: 0.28% (93)
RFID: 0.01% (4)
NFC: 0.03% (10)
Smartcard: 0.00% (1)
BIOS: 0.25% (82)
CMOS: 0.01% (3)
Southbridge: 0.00% (0)
Northbridge: 0.00% (0)
TPM: 0.02% (7)
VRM: 0.01% (4)
PLL: 0.01% (2)
M.2: 0.00% (0)
PS/2 Port: 0.00% (0)
Audio Codec Chip: 0.00% (0)
ADC: 0.29% (97)
DAC: 0.16% (52)
Thermocouple: 0.00% (0)
Fan Controller: 0.00% (0)
BSP: 0.06% (21)
VME: 0.03% (9)
VPX: 0.01% (2)
cPCI: 0.02% (6)
zigbee: 0.01% (3)
mqtt: 0.09% (31)
uart: 0.04% (12)
jtag: 0.00% (0)
firmware: 0.99% (325)
u-boot: 0.01% (2)
microkernel: 0.02% (7)
MCU: 0.01% (2)
MPU: 0.28% (93)
MMU: 0.74% (244)
disk: 0.18% (58)
SSD: 0.05% (15)
nvme: 0.02% (5)
1553: 0.00% (1)
spacewire: 0.00% (0)
smbus: 0.00% (0)
SDIO: 0.00% (1)
MDIO: 0.00% (0)
ACPI: 0.01% (3)
microcode: 0.00% (0)
SGX: 0.01% (4)
Intel Management Engine: 0.00% (0)
Trusted Platform Module: 0.01% (3)
Intel Platform Trust Technology: 0.00% (0)
PTT: 0.01% (2)
Intel Software Guard Extensions: 0.00% (0)
Intel Trusted Execution Technology: 0.00% (0)
TXT: 0.11% (35)
Intel Speed Shift Technology: 0.00% (0)
Intel Turbo Boost Technology: 0.00% (0)
Intel Quick Sync Video: 0.00% (0)
Intel Optane Memory: 0.00% (0)
Cortex-M: 0.00% (0)
Cortex-A: 0.00% (1)
Security Processing Unit: 0.00% (0)
SPU: 0.18% (59)
Platform Security Architecture: 0.00% (0)
PSA: 0.02% (8)
CryptoCell: 0.00% (1)
Confidential Computing Architecture: 0.00% (0)
CCA: 0.02% (6)