
2019 PRODUCT SECURITY REPORT
Intel Product Assurance and Security

Intel provides these materials as-is, with no express or implied warranties.

All products, dates, and figures specified are preliminary, based on current expectations, and are subject to change without notice.

Intel, processors, chipsets, and desktop boards may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at http://intel.com.

Some results have been estimated or simulated using internal Intel analysis or architecture simulation or modeling, and provided to you for informational purposes. Any differences in your system hardware, software or configuration may affect your actual performance.

CONTENTS

Foreword 5
Key Findings 7
Industry Collaboration 9
Investing in Security Research 11
Bug Bounty Program 13
CVEs by Category and Severity 15
Microprocessor Vulnerabilities 21

FOREWORD

FOREWORD

2019 was a year of continued leadership in security assurance. We continued to forge collaborative partnerships across the industry to drive initiatives to build the foundation of trusted computing. Our unparalleled focus on relationships and transparency with security researchers and the most advanced technology companies in the world, continues to be one of our greatest assets and we will continue our efforts into 2020 and beyond.

Long before we made our Security First pledge, Intel has had a systematic approach to addressing product vulnerability reports whether found by the external research community or found internally by Intel employees. It is, and has been, our goal to assign Common Vulnerability and Exposures (CVE) identification numbers to product vulnerabilities across tens of thousands of products, and assist our customers in risk analysis by publishing security advisories to the Intel Security Center.

Through our continued investment in product security research, in 2019, 144 of the 236 CVEs (61%) published were discovered internally by Intel employees. We believe documenting and publicizing internally found vulnerabilities provides a critical level of transparency to our customers.

Of the 92 vulnerabilities reported by external researchers, 70 (76%), were reported to Intel through our Bug Bounty program. Through the terms of our Bug Bounty program, there is a much higher assurance of Coordinated Vulnerability Disclosure (CVD) but even so, in almost every externally reported case, researchers coordinated with Intel through the vulnerability management process to the eventual public disclosure.

Combining Bug Bounty and internally found vulnerabilities, the data shows that 91% of the issues addressed are the direct result of Intel's investment in product assurance. None of the 236 vulnerabilities addressed in 2019 were known to be used in actual attacks at the time of public disclosure.

A little more than half of the public disclosures in 2019 were part of the Intel Platform Update (IPU) process through which security and functional updates are bundled by platform. These bundles may include microcode, firmware, and software updates and are provided to Intel partners for validation and integration so that the entire ecosystem from operating system, hypervisor, original equipment manufacturers (OEMs), Cloud Service Providers, and others, are ready to provide these mitigations to customers at the time of public disclosure. The rest of the issues were released as part of our monthly update process which aligns to the second Tuesday of each month along with many others in the industry.

CPU level vulnerabilities in 2019 equated to only 5% (11) of the overall CVE count and carried an average CVSS score of 5.02 for the year. As acknowledged by security researchers and industry experts, side-channel issues are difficult to exploit and often require a level of access to the target system that would afford would be attackers more efficient and reliable methods of obtaining and exfiltrating information.

In 2019, 144 of the 236 CVEs (61%) published were discovered internally by Intel employees.

Of the 92 vulnerabilities reported by external researchers, 70 (76%), were reported to Intel through our Bug Bounty program.

91% of all vulnerabilities addressed are the direct result of Intel's investment in product assurance.

CPU level vulnerabilities in 2019 equated to only 5% (11) of the overall CVE count in 2019.

None of the 236 vulnerabilities addressed in 2019 were known to be used in actual attacks at the time of public disclosure.

KEY FINDINGS

KEY FINDINGS

At Intel, we have made significant investments in product assurance and security, especially when it comes to the proactive discovery and mitigation of product vulnerabilities. Our investments in internal research and externally through our Bug Bounty program accounted for 91% of all CVEs disclosed in 2019. A key aspect of our bug bounty program is adherence to industry best practices for Coordinated Vulnerability Disclosure (CVD) – the intent of which is help protect users from unmitigated security vulnerabilities. All vulnerabilities disclosed through our Bug Bounty program in 2019 occurred on dates mutually agreeable to Intel and the security researchers who reported them. These dates were informed by availability of mitigations and with input from our customers and partners in the industry.

- 61% (144 of 236) of CVEs addressed in 2019 were found internally through Intel's research efforts.
- Of the 92 externally reported vulnerabilities, 70 (76%) were reported through Intel's Bug Bounty program.
- 91% of vulnerabilities addressed were the direct result of Intel's investment in ongoing product assurance (internally found + Bug Bounty).
- 61% of High severity vulnerabilities and 75% of Critical severity vulnerabilities were found internally by Intel.
- 11 CPU issues were addressed in 2019.


INDUSTRY COLLABORATION

INDUSTRY COLLABORATION

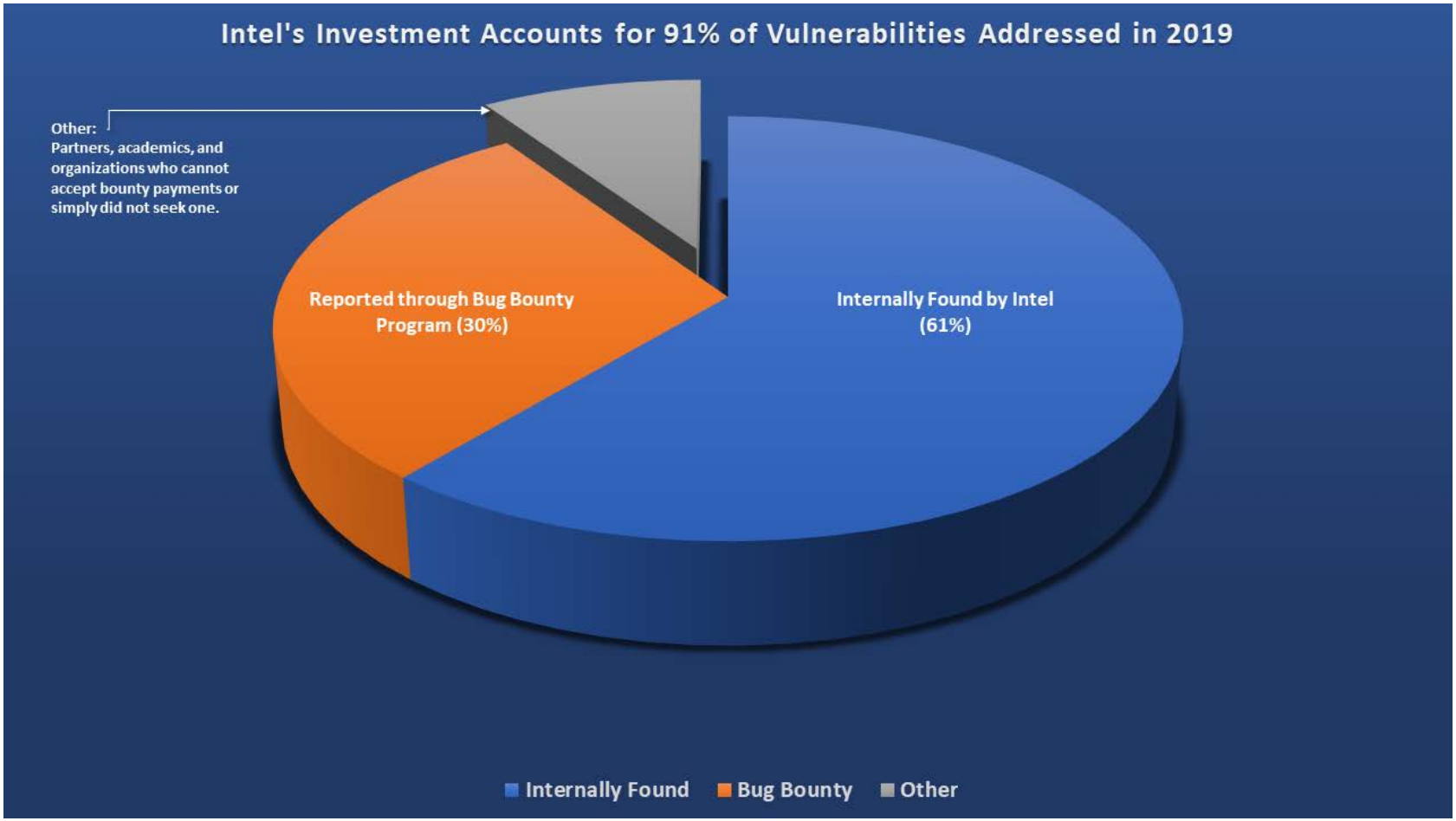
Powering our data-centric world requires cross-industry collaboration to build a future of innovation and security. Intel works with partners, competitors, customers, and across sectors to identify and proactively address potential threats.

At Intel, our Security First Pledge means that we set aside competitive differences to enhance the security of our customers, and even that of our competitors. We engage in cross-industry collaboration that aids in the development of future security technologies and the creation of innovative security mitigations. We know that our products, whether in the data center, on the edge, or on the desktop, are built on a foundation of trust.

Industry collaboration is a key and strategic component to how we seek to lead in hardware security innovation. Every day we collaborate with the leading operating system, hypervisor, and cloud services providers, to work on microarchitectural solutions that have impact on a global scale. It is truly amazing when companies, some of which may be competitors in the global market place, can work together on solutions that benefit the entire ecosystem.


INVESTING IN SECURITY RESEARCH

INVESTING IN SECURITY RESEARCH



Publishing information about internally found vulnerabilities helps customers more accurately assess impact and risk.

91% of all vulnerabilities addressed in 2019 were the direct result of Intel's investments in vulnerability research and product assurance.

Putting a priority on discovering and reporting internally found vulnerabilities is a reflection of the advanced level* of maturity of Intel's vulnerability management program. The success of our Bug Bounty program is demonstrated by the fact that 76% of the externally reported issues came through the program.

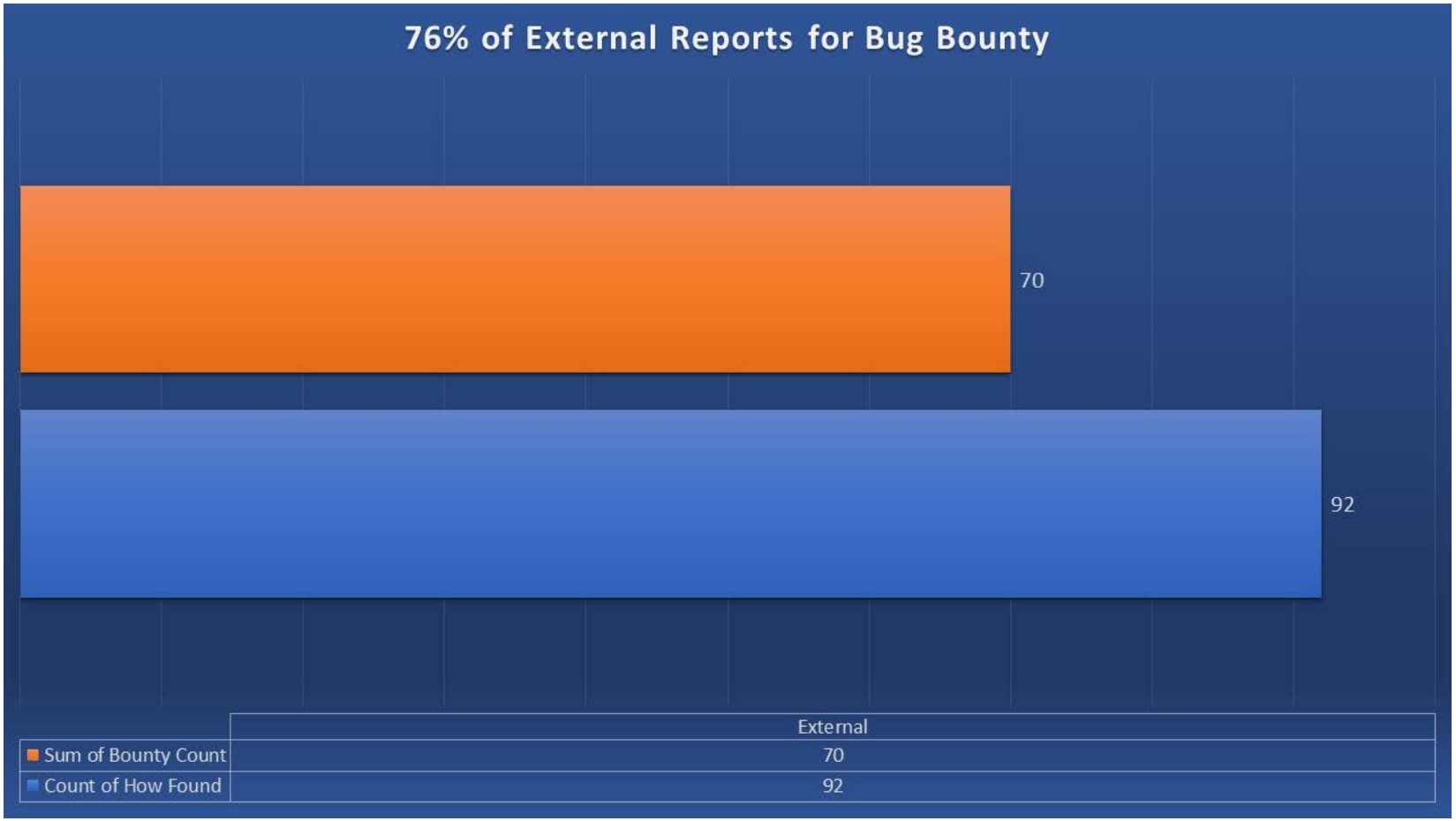
** See the FIRST.org PSIRT Maturity Document: https://www.first.org/education/PSIRT-maturity-document.pdf*


BUG BOUNTY PROGRAM

BUG BOUNTY PROGRAM

Intel believes that working with skilled security researchers across the globe is a crucial part of identifying and mitigating security vulnerabilities in Intel products.

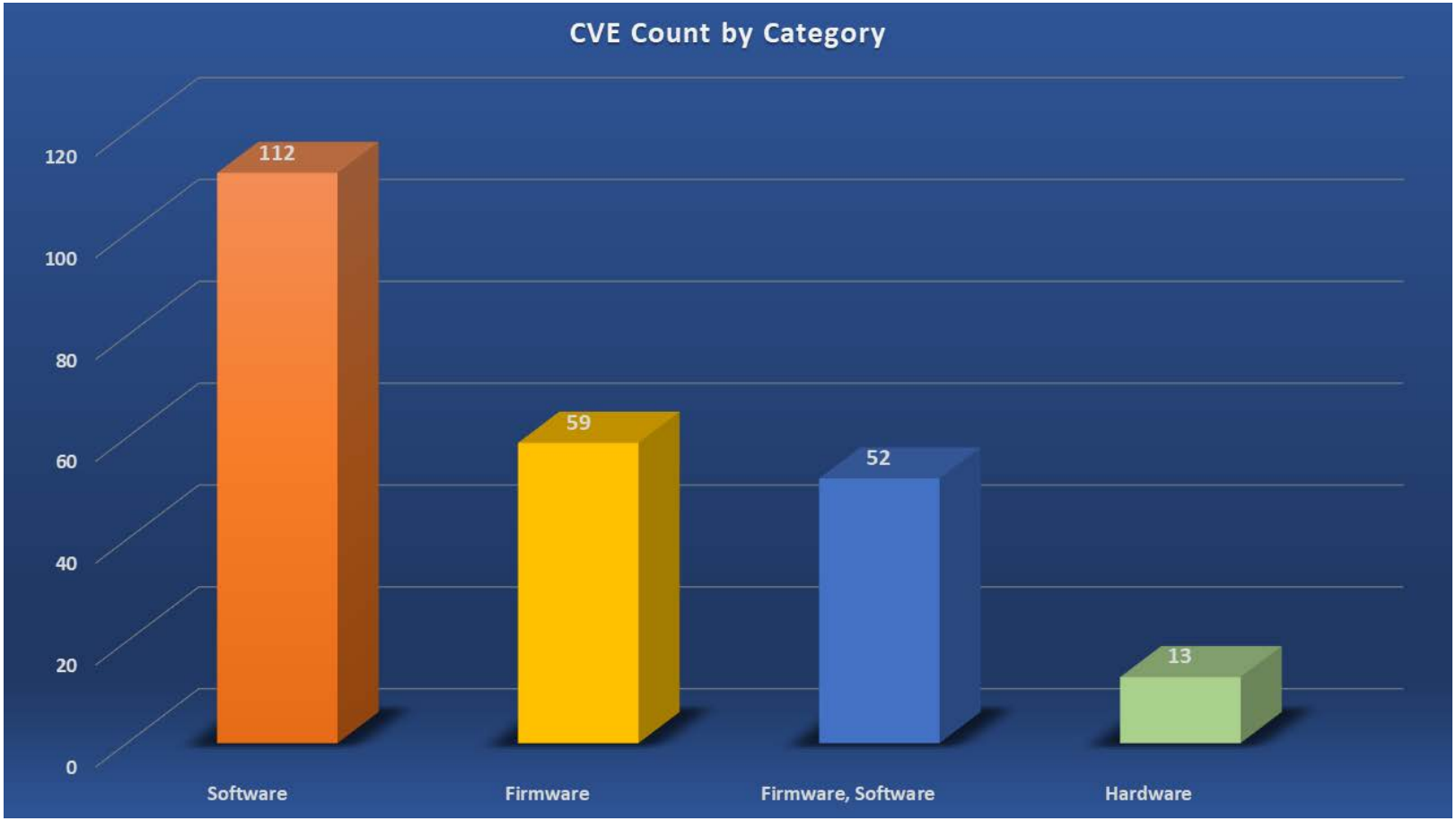
Like other major technology companies, Intel incentivizes security researchers to report security vulnerabilities in Intel products. This helps us enable a coordinatedresponse. To encourage closer collaboration with the security research community on these kinds of issues, Intel created its Bug Bounty Program. Of the 92 CVEs addressed in 2019 that were reported by external security researchers, 70 (76% of external reports and 30% of the overall total) were reported through our Bug Bounty program. We appreciate these researchers not only for their talent but also for coordinating with us to help ensure mitigations are available to customers ahead of public disclosure.




CVE CATEGORIES & SEVERITY

CVES BY CATEGORY AND SEVERITY

Intel Security Advisories are broken down by three primary categories: software, firmware, and hardware. In some cases, a complete mitigation may require a software driver update and a firmware update, so this combination is called out separately in the chart below.



Further breakdown of categories:

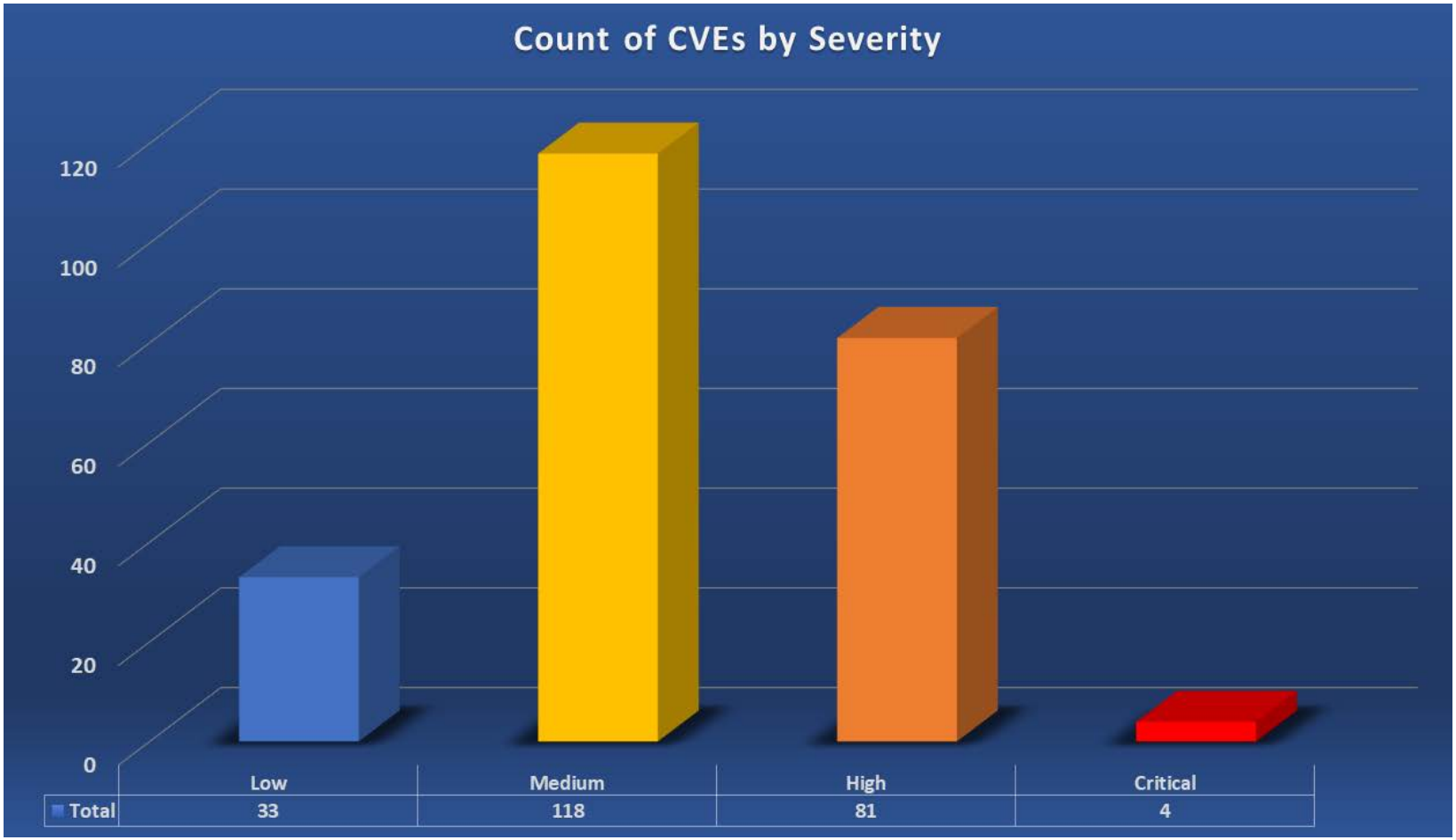
Software includes:
Software only driver updates
Applications
Utilities
Etc.

Firmware includes:
Intel(R) Management Engine
BOIS/UEFI
Authenticated Code Module (ACM)
Networking product firmware
Graphics firmware
Etc.

Firmware and Software includes:
Instances where the above software and firmware updates are delivered together to mitigate an issue.

Hardware includes:
Microcode updates

Of the CVEs identified, almost two thirds (151 of 236, or 64%) were of low or medium severity, and the remaining (81 of 236, or 34%) were of high severity. Only 4 of 236 CVEs, less than 2%, were of critical severity.

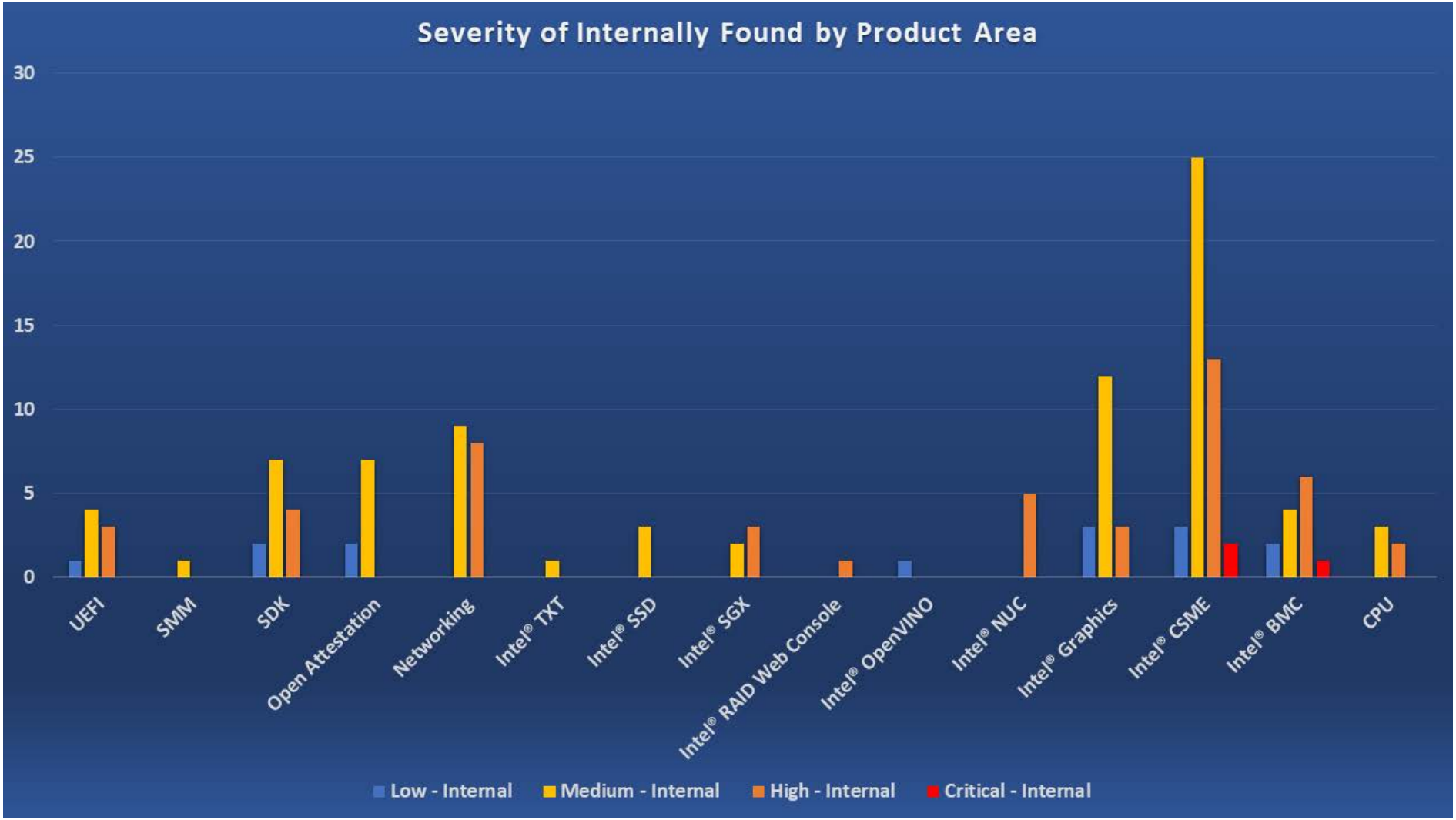


The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments, the Temporal group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics.

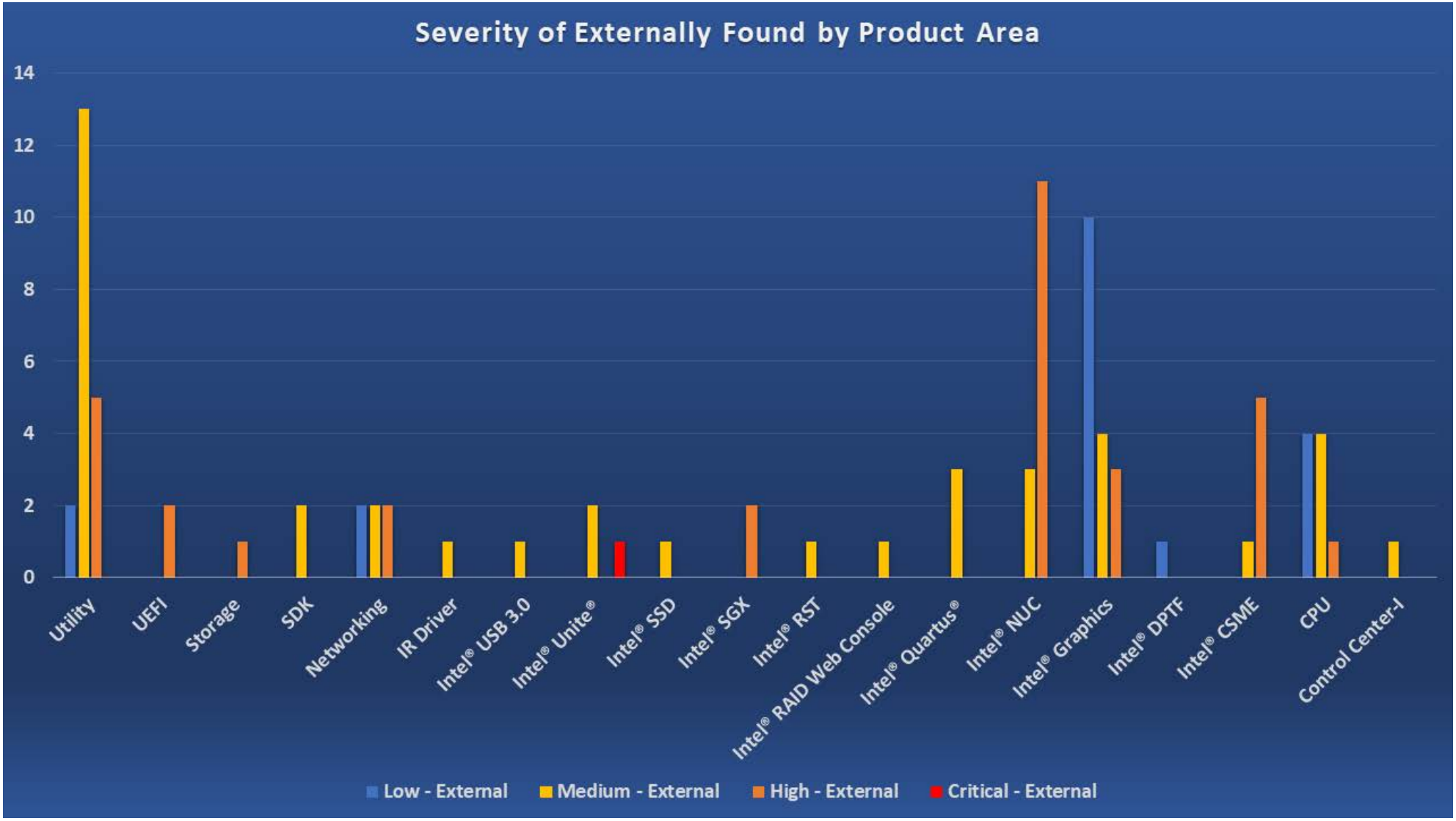
CVSS severity scores fall into five categories:

None: 0.0
Low: 0.1 - 3.9
Medium: 4.0 - 6.9
High: 7.0 - 8.9
Critical: 9.0 - 10.0

For information on the Common Vulnerability Scoring System, visit: https://www.first.org/cvss/

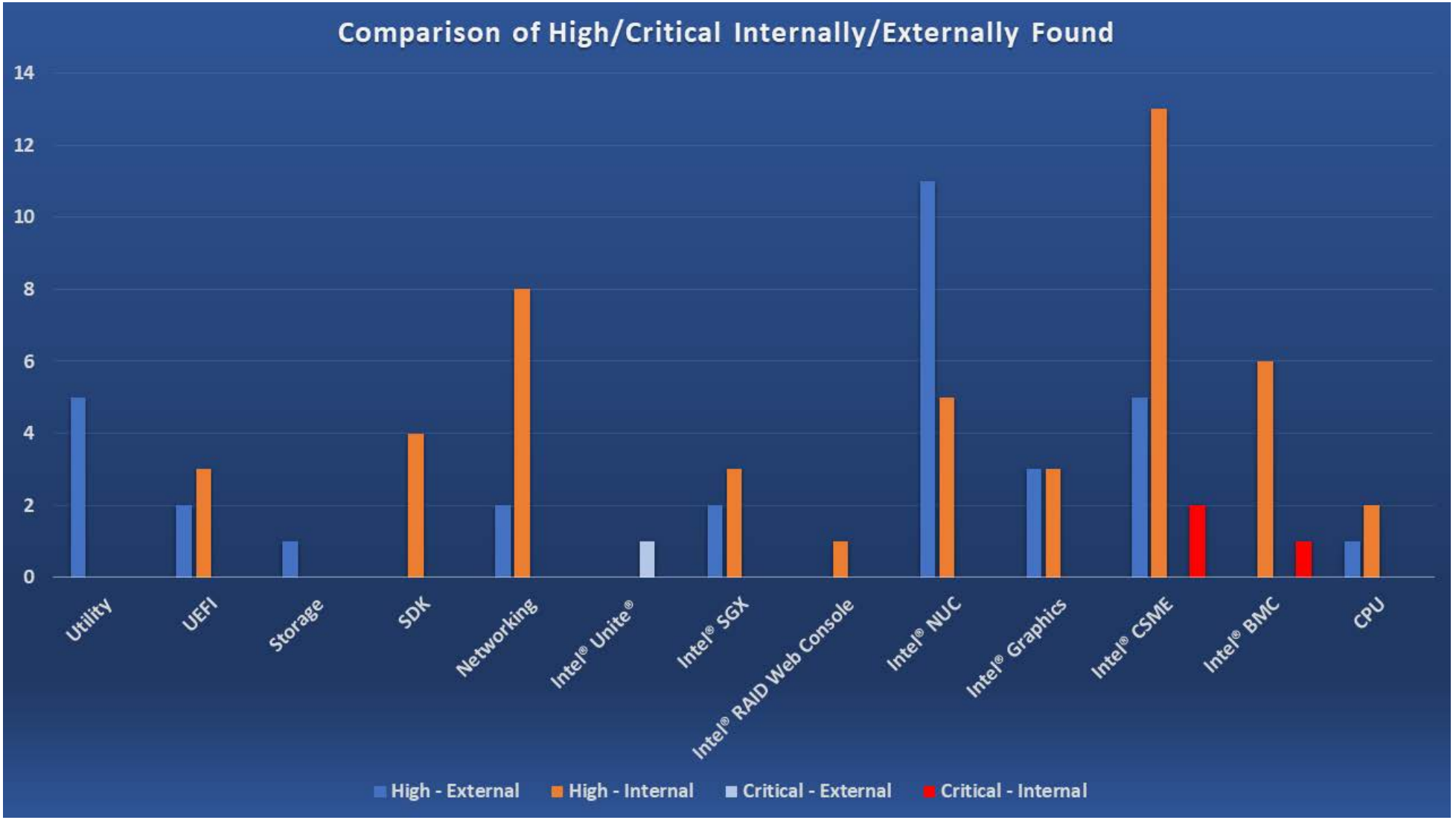


The majority of High and Critical severity issues were found internally by Intel. As part of Intel's commitment to transparency, these issues were assigned CVE ID's and publicly reported through our security advisories at https://intel.com/security.



As stated, the majority of externally found issues were reported to Intel through our Bug Bounty program. The majority of the externally reported issues were in software components including various utilities and drivers. We appreciate the work of the security research community and look forward to ongoing engagement through our bounty program in 2020.

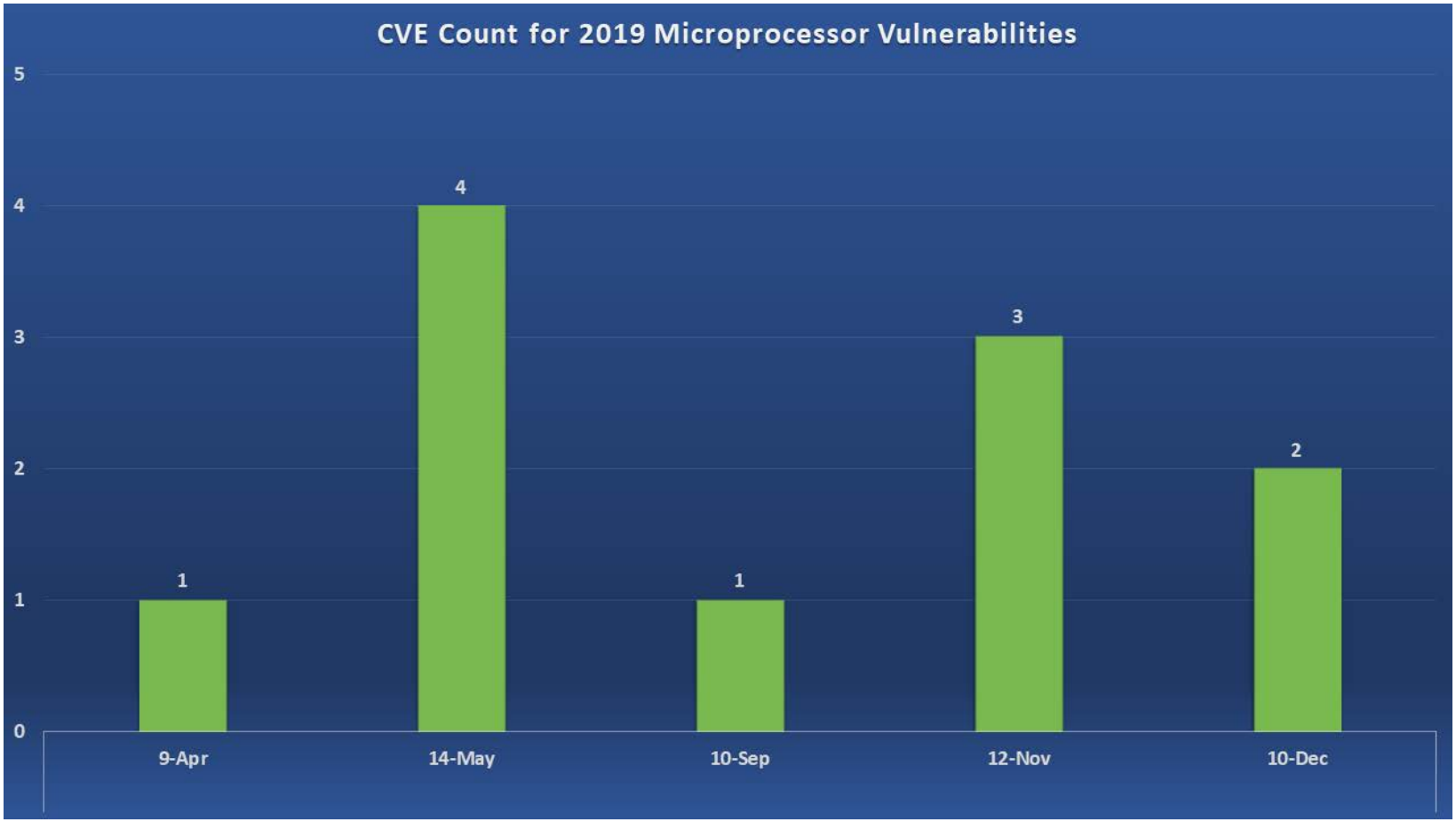
The final chart in this section shows a side by side comparison of internally and externally found High and Critical severity vulnerabilities. 61% of High severity vulnerabilities and 75% of Critical severity vulnerabilities were found internally by Intel.



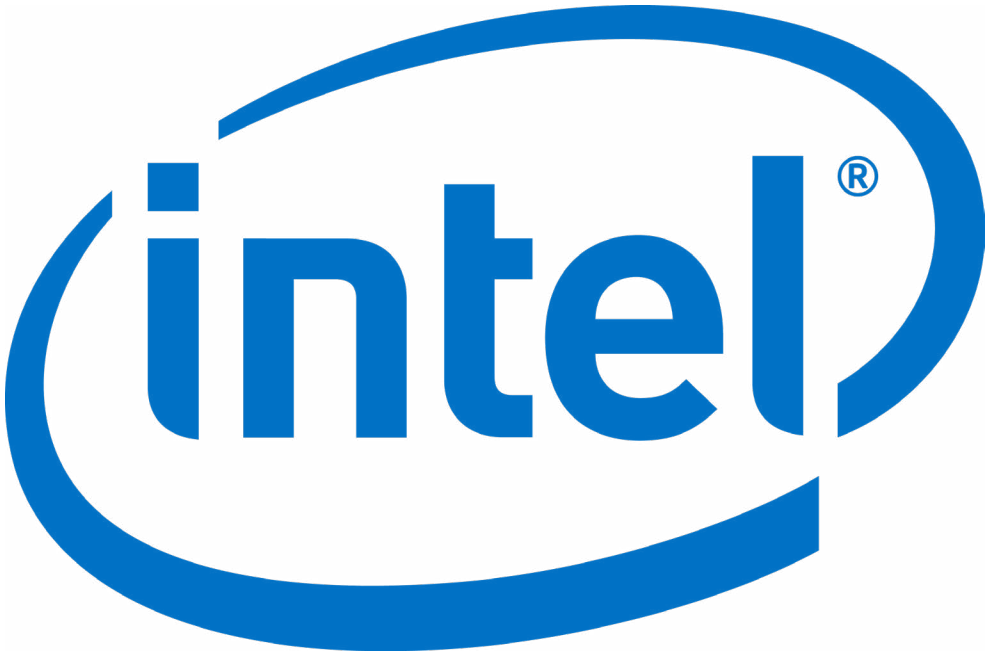

MICROPROCESSOR VULNERABILITIES

MICROPROCESSOR VULNERABILITIES

In 2019, Intel mitigated 11 microprocessor vulnerabilities, representing 5% of the overall CVE count for the year. These microarchitectural side channel vulnerabilities are often closely related, generally difficult to exploit and to Intel's knowledge, have not been successfully utilized outside of a controlled lab environment at the time of this report. Intel works to address these vulnerabilities in a timely manner when they are identified by internal or external security researchers, and we have great appreciation for the dedication and talent required for their discovery.



In 2019, Intel mitigated 11 microarchitectural side channel vulnerabilities, representing 5% of the total issues mitigated.


intel