Microsoft, Intel issue urgent warnings about MMIO Stale Data vulnerability on Windows 11, 10

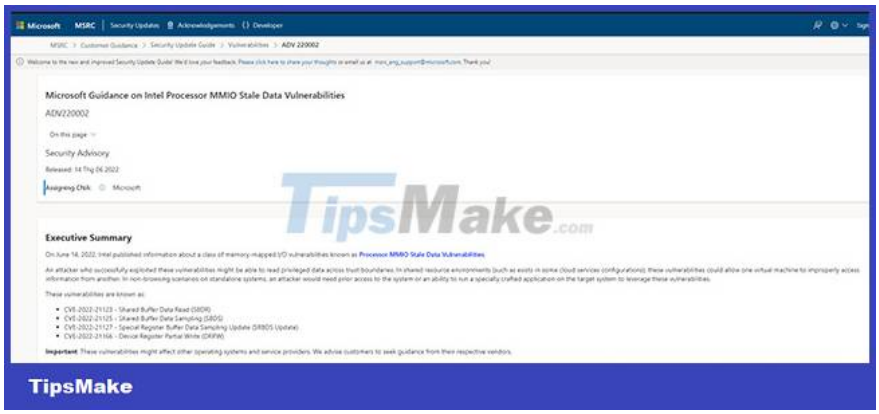
Intel and Microsoft have just rushed to publish a list of security advisories related to a series of new CPU vulnerabilities affecting Intel Core processors.

These security flaws are related to the memory mapped I/O (MMIO) component of the CPU, and are therefore collectively known as "MMIO Stale Data Vulnerabilities". After successfully abusing a vulnerable system, a threat actor can simply read privileged information on the system.

In the recently released ADV220002 security advisory document, Microsoft describes the following potential attack scenarios:

> 'An attacker who successfully exploited these vulnerabilities could read privileged data on the system across trust boundaries. In shared resource environments (such as in some cloud service configurations), these vulnerabilities could allow one virtual machine to improperly access information from another. Given the situation on standalone systems, an attacker would need prior access to the system or the ability to run a specially designed application on the target system to take advantage of these vulnerabilities.
>
> The list of vulnerabilities that have been documented and tracked includes:

1. CVE-2022-21123 - Shared Buffer Data Read (SBDR)
2. CVE-2022-21125 - Shared Buffer Data Sampling (SBDS)
3. CVE-2022-21127 - Special Register Buffer Data Sampling Update (SRBDS Update)
4. CVE-2022-21166 - Device Register Partial Write (DRPW)



MMIO uses the processor's physical memory address space to access I/O devices, which can respond as memory elements. According to the security advisory document INTEL-SA-00615, Intel has also described in more detail how the vulnerability can be exploited using the CPU's uncached cache data:

> The MMIO Stale Data vulnerabilities are a type of memory-mapped I/O (MMIO) vulnerability that can expose data. When a processor core initiates an MMIO read or write process, the transaction is typically performed with non-storable or write-associated memory types and is passed through non-volatile memory, which is a logical part in the shared CPU. shared by the processor cores and provides a number of common services.
>
> [.] These vulnerabilities involve a series of operations that result in stale data being read directly into the architecture, software-visible state, or sampled from buffers or registers. In some attack cases, stale data may already be in the microarchitecture cache. For other attack scenarios, malicious actors can transfer data from microarchitecture locations such as fill buffers.

Analysis from Microsoft shows that the following versions of Windows may be affected by the vulnerability:

1. Windows 11
2. Windows 10
3. Windows 8.1
4. Windows Server 2022
5. Windows Server 2019
6. Windows Server 2016

The list of affected CPUs along with the corresponding mitigation measures are given as follows:

Table 1: Processor MMIO Stale Data Vulnerability Summary

Name (Acronym)	CVE (CVSS)	Affected Products	Privilege Required	Data Exposure	Mitigation Direction	Software Proposal
Device Register Partial Write (DRPW)	CVE-2022-21166 (5.5 Medium: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)	• Intel® Xeon® Scalable processor family • Client • Intel® Xeon® E3 processor family	MMIO	fill buffers, uncore buffers	microcode and software (same Simultaneous Multi-Threading restrictions as MDS)	Software buffer overwriting if untrusted software has MMIO access
Update to Special Register Buffer Data Sampling (SRBDS Update)	CVE-2022-21127 (5.5 Medium: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)	• Client • Intel Xeon E3 processor family	Ring 3	RDRAND, RDSEED, SGX EGETKEY	microcode	Same as SRBDS
Shared Buffers Data Read (SBDR)	CVE-2022-21123 (6.1 Medium: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N)	• Client • Intel Xeon E3 processor family	MMIO	RDRAND, RDSEED, SGX EGETKEY, fill buffers, uncore buffers	microcode and software	Software buffer overwriting if untrusted software has MMIO access
Shared Buffers Data Sampling (SBDS)	CVE-2022-21125 (5.6 Medium: AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N)	• Client • Intel Xeon E3 processor family	Ring 3, MMIO	fill buffers, uncore buffers	microcode and software	Software buffer overwriting if untrusted software has MMIO access

The full list of affected CPU models can be found on Intel's official website, in the 2022 section.

You finished reading the article "**Microsoft, Intel issue urgent warnings about MMIO Stale Data vulnerability on Windows 11, 10**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.