



Cytex Research

CVE-2022-40982
Intel® Downfall Vulnerability

Intel Downfall Vulnerability Advisory

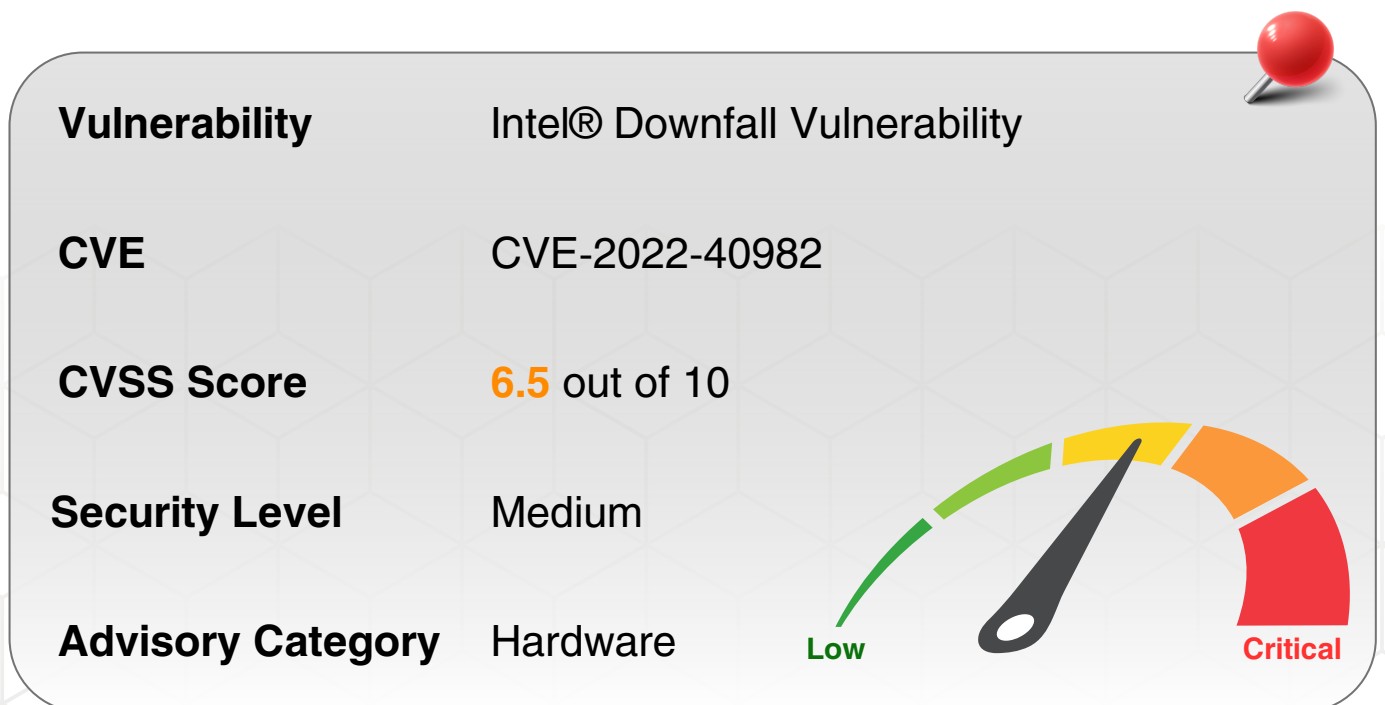
hello@cytex.io | <https://cytex.io>

1

What is the Downfall vulnerability and why should I care?

The Downfall vulnerability was discovered by Google researchers in 2022 and tracked by CVE-2022-40982. The researchers waited for almost 1 year before disclosing it to allow the vendor time to develop a remediation patch.

Downfall vulnerability is a side-channel attack that allows a malware or an attacker to obtain sensitive information from the targeted device. All Intel Core and Xeon processors released over the last decade that are based on Skylake through Ice Lake microarchitecture are impacted by this vulnerability. Downfall's impact is going to be felt throughout the industry because of the massive adoption of Intel processors in desktops, laptops, and servers including cloud hosted servers. Since cloud environments are also impacted, it may be possible to launch remote attacks, even though a remote exploit has not yet been released.



2 How does the Downfall attack work?

Downfall vulnerability exploits a flaw in the memory optimization feature found in Intel processors. The attack leverage two techniques: Gather Data Sampling (GDS) and Gather Value Injection (GVI). Gather instructions are part of a memory optimization and the attack exploits this instruction to leak the contents of the internal vector register file.

3 How do I know if I am at risk?

The following Intel processor families are at risk:

- Skylake, Cascade Lake, Cooper Lake, Amber Lake, Kaby Lake, Coffee Lake, Whiskey Lake, Comet Lake
- Tiger Lake
- Ice Lake, Rocket Lake

If your local server, device, or cloud environment uses any of the affected processor families, then you may be at risk.

Furthermore, if you use cryptographic libraries such as OpenSSL, you may be at risk. OpenSSL uses the accelerated implementation of cryptographic primitive functions using x86 SIMD instructions, there is an elevated risk that an attacker may extract cryptographic keys and plaintexts that are processed with the SIMD instructions.



Your computing devices (laptop, tablet, desktop, cloud, etc.) based on Intel Core processors from the 6th Skylake to (including) the 11th Tiger Lake generation are affected.



The vulnerability presents an opportunity for malicious actors to exploit an information leak, potentially compromising sensitive data such as private messages, passwords, and encryption keys.

4

What should I do?

You should perform these actions to mitigate the impact of the Downfall vulnerability. The software-based mitigation disables the Gather instructions, which is likely to cause performance degradation.

Note: If you are a Cytex EDR customer, you can readily identify the operating system version for all your managed devices as well as the system libraries installed on those devices. You can also use the Cytex SBOM inventory report to identify installed libraries. Both reports can be used to identify the affected devices and software libraries.

1. Identify all your managed devices that contain the affected processor families and update the microcode. Intel's microcode update is available at: <https://github.com/intel/Intel-Linux-Processor-Microcode-Data-Files>
2. Many operating systems have incorporated the update so you should update to the latest operating version. See the Vendor Advisory section for a list of the advisories.
3. Identify the current version of OpenSSL installed on your devices and update to the latest version.
4. Identify any libraries linked with OpenSSL and update or recompile them with the latest OpenSSL version.



Update the microcode: Intel's microcode update thwarts attacker access to speculative data from Gather instructions.



Update to the latest OpenSSL version and update/recompile any linked libraries.



Update your operating system to the latest version; consult the Vendor Advisory section for advisories.

5

Vendor Advisories

- Intel Security Advisory INTEL-SA-00828
 - <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00828.html>
- Debian DSA-5474-1
 - <https://www.debian.org/security/2023/dsa-5474>
- Debian DSA-5475-1
 - <https://www.debian.org/security/2023/dsa-5475>
- FEDORA-2023-10d34be85a
 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/HKREYYTWUY7ZDNIB2N6H5BUJ3LE5VZPE/>
- FEDORA-2023-e1482687dd
 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OL7WI2TJCWSZIQP2RIOLWHOKLM25M44J/>
- FEDORA-2023-fff31650c8
 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/T7WO5JM74YJSYAE5RBV4DC6A4YLEKWLF/>
- Downfall page: <https://downfall.page/>
- Red Hat: Gather Data Sampling (GDS) (also known as “Downfall”)
 - <https://access.redhat.com/solutions/7027704>
- AWS
 - <https://aws.amazon.com/security/security-bulletins/AWS-2023-007/>
- Xen Security Advisory CVE-2022-40982 / XSA-435
 - <https://xenbits.xen.org/xsa/advisory-435.html>
- MLIST: Debian LTS Advisory DLA-3525-1
 - <https://lists.debian.org/debian-lts-announce/2023/08/msg00013.html>
- MLIST: Debian LTS Advisory DLA-3537-1
 - <https://lists.debian.org/debian-lts-announce/2023/08/msg00026.html>



cytex-inc



@cytexsmb



@cytexsecure