مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Intel

Tracking #:432316151

Date:15-08-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Intel has released security advisories addressing multiple vulnerabilities in its products.

TECHNICAL DETAILS:

Vulnerability Details (Including but not limited to):

- **CVE-2024-21810** | Base Score: 8.8 High
  - Improper input validation in the Linux kernel mode driver for some Intel® Ethernet Network Controllers and Adapters before version 28.3 may allow an authenticated user to potentially enable escalation of privilege via local access.
  - **Affected Products**: Intel(R) Ethernet Complete Driver Pack before version 28.3.

- **CVE-2024-23497** | Base Score: 8.8 High
  - Out-of-bounds write in Linux kernel mode driver for some Intel® Ethernet Network Controllers and Adapters before version 28.3 may allow an authenticated user to potentially enable escalation of privilege via local access.
  - **Affected Products**: Intel(R) Ethernet Complete Driver Pack before version 28.3.

- **CVE-2024-25576** | Base Score: 7.9 High
  - Improper access control in firmware for some Intel(R) FPGA products before version 24.1 may allow a privileged user to enable escalation of privilege via local access.
  - **Affected Products**: Intel Agilex® FPGA 7 FPGA firmware before version 24.1.

- **CVE-2023-42667** | Base Score: 7.8 High
  - Improper isolation in the Intel® Core™ Ultra Processor stream cache mechanism may allow an authenticated user to potentially enable escalation of privilege via local access.
  - **Affected Products**: Intel® Core™ Ultra processors Meteor Lake Client

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to install fixed version released by Intel at the earliest.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00918.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01022.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01038.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01046.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01070.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01083.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01087.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01121.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01172.html