LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF INFORMATION SECURITY

HC3: Sector Alert

November 16, 2021 TLP: White Report: 202111161700

Intel BIOS Vulnerabilities

Executive Summary

Intel recently disclosed two high-severity vulnerabilities that affect several of their processor families. Both of these allow for a potential escalation of privilege attack. These processors are included in systems widely deployed across many industries, including the healthcare and public health sector. HC3 recommends all healthcare organizations apply vendor-provided patches to vulnerable systems in a timely and comprehensive manner.

Report

Intel has disclosed two high-severity vulnerabilities that affect Pentium, Celeron and Atom processors of the Apollo Lake, Gemini Lake and Gemini Lake Refresh platforms. The specific list of processors is as follows:

- Intel Xeon Processor E Family
- Intel Xeon Processor E3 v6 Family
- Intel Xeon Processor W Family
- 3rd Generation Intel Xeon Scalable Processors
- 11th Generation Intel Core™ Processors
- 10th Generation Intel Core™ Processors
- 7th Generation Intel Core™ Processors
- Intel Core™ X-series Processors
- Intel Celeron Processor N Series
- Intel Pentium Silver Processor Series

Analysis

These processors are widely used across many industries including the healthcare and public health sector. Therefore, HC3 recommends all healthcare organizations examine the list of vulnerable processors (above) against an updated IT asset inventory to identify any vulnerable systems that may need to be patched.

Vulnerabilities

They vulnerabilities are tracked as CVE-2021-0157 and CVE-2021-0158, with each having a CVSS score of 8.2 out of 10.

Patches, Mitigations, and Workarounds

For any enterprise that identifies a vulnerable system, Intel recommends installing the UEFI BIOS updates published by the end manufacturers of the respective electronic equipment. Also, Intel is in the process of releasing firmware updates to mitigate these vulnerabilities. Intel's Support and Downloads site can be found at: https://www.intel.com/content/www/us/en/support.html

References

INTEL-SA-00562: BIOS Reference Code Advisory
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html

Intel: Support and Downloads
https://www.intel.com/content/www/us/en/support.html

Intel chip flaw could enable attacks on laptops, cars, medical devices (CVE-2021-0146)
https://www.helpnetsecurity.com/2021/11/15/intel-chip-flaw-cve-2021-0146/

High severity BIOS flaws affect numerous Intel processors
https://www.bleepingcomputer.com/news/security/high-severity-bios-flaws-affect-numerous-intel-processors/

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback