مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in HP Insyde BIOS

Tracking #:432317846

Date:22-10-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that HP has identified a high-severity vulnerability in certain ARM-based HP PC products utilizing InsydeH20 UEFI firmware. The flaw could allow arbitrary code execution by an attacker with local administrative privileges.

TECHNICAL DETAILS:

A high-severity security vulnerability has been discovered in certain ARM-based HP PCs utilizing Insyde BIOS (InsydeH20 UEFI Firmware). The vulnerability, tracked as CVE-2022-35407, could allow an attacker with appropriate privileges to execute arbitrary code with elevated permissions. This poses a significant security risk and could lead to system compromise.

Vulnerability Details

- **CVE-2022-35407**
- CVSS v3.1 Base Score: 7.7 (High)
- A flaw in the Insyde BIOS firmware could allow an attacker to execute arbitrary code during system initialization or BIOS runtime by exploiting improper code handling in firmware components.
- **Potential Impact:** Arbitrary code execution within system firmware, potentially compromising device integrity and security.

Affected Products and Fixed Versions

This vulnerability affects select ARM-based consumer notebook PCs using Qualcomm platforms and Insyde BIOS firmware, including the following models:

- HP OmniBook X 14" Laptop AI PC (14-fe0xxx) – BIOS version F.32 or later (SoftPaq SP162865)
- HP OmniBook X 14" Laptop Next Gen AI PC (14-fe1xxx) – BIOS version F.22 or later (SoftPaq SP162866)
- HP EliteBook Ultra G1q 14" Notebook AI PC – BIOS version F.32 or later (SoftPaq SP162865)
- HP EliteBook Ultra G1q8 14" Notebook AI PC – BIOS version F.22 or later (SoftPaq SP162866)

RECOMMENDATIONS:

- Ensure BIOS/firmware is updated to the latest available version.
- Maintain up-to-date drivers and operating system patches.
- Restrict administrative privileges to trusted users only.
- Regularly monitor HP’s Security Bulletin page for future updates or advisories.

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://support.hp.com/si-en/document/ish_13143750-13143772-16/hpsbhf04067