مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical BIOS Vulnerabilities Impacting Lenovo Desktops

Tracking #:432317559

Date:01-08-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed critical BIOS vulnerabilities impacting Lenovo desktops. These flaws could allow attackers with elevated privileges to execute arbitrary code in System Management Mode (SMM)—a highly privileged CPU execution mode—potentially leading to full system compromise.

TECHNICAL DETAILS:

Multiple critical vulnerabilities have been identified in the InsydeH2O BIOS firmware used in Lenovo IdeaCentre AIO 3 and Yoga All-in-One desktop series. These flaws impact System Management Mode (SMM), allowing local attackers with administrative privileges to execute arbitrary code with firmware-level privileges or read sensitive memory, potentially resulting in persistent system compromise.

Vulnerability Details:

CVE ID	CVSS Score	Description
CVE-2025-4421	8.2	SMM memory corruption (gEfiSmmCpuProtocol)
CVE-2025-4422	8.2	SMM memory corruption (EfiPcdProtocol)
CVE-2025-4423	8.2	Arbitrary code execution (SetupAutomationSmm)
CVE-2025-4424	6.0	Unsanitized input (SmmSetVariable calls)
CVE-2025-4425	8.2	Stack overflow (SMI handler)
CVE-2025-4426	6.0	Information Exposure (SMRAM disclosure)

Impact:
These vulnerabilities could allow attackers with local administrative access to:

- Read or modify sensitive firmware memory (SMRAM)
- Execute arbitrary code at the firmware level
- Permanently compromise the integrity of the operating system and installed security controls

Affected Systems and Mitigations:

- IdeaCentre AIO 3 (24ARR9, 27ARR9) – Minimum fixed BIOS version: O6BKT1AA
- Yoga AIO (27IAH10, 32ILL10, 9 32IRH8) – BIOS fixes scheduled for phased release (Sep–Nov 2025)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Vendor.

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.lenovo.com/in/en/product_security/LEN-201013