مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Local Privilege Escalation Vulnerability in HPE SimpliVity Servers

Tracking #:432317808

Date:13-10-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Hewlett Packard Enterprise (HPE) has released a security update addressing a local privilege escalation vulnerability (CVE-2025-20109) affecting certain HPE SimpliVity Gen11 servers that use impacted Intel processors.

TECHNICAL DETAILS:

Hewlett Packard Enterprise (HPE) has released a security update addressing a local privilege escalation vulnerability (CVE-2025-20109) affecting certain HPE SimpliVity Gen11 servers that use impacted Intel processors.

The flaw originates from the Intel Processor Stream Cache component, disclosed under Intel Security Advisory INTEL-SA-01249 as part of the 2025.2 Intel Platform Update (IPU). Successful exploitation may allow a local attacker with limited privileges to escalate privileges on the affected system, potentially compromising system confidentiality, integrity, and availability.

Vulnerability Details:

- CVE: CVE-2025-20109
- Severity (CVSS v3.1): 7.8 (High
- Description: Intel Processor Stream Cache vulnerability (described in Intel advisory INTEL-SA-01249) that can be abused for local privilege escalation on affected HPE SimpliVity systems.
- Affected product / versions: HPE SimpliVity 380 Gen11 — firmware prior to HPE SimpliVity Gen11 Firmware v2025_1001.
- Fixed version- HPE SimpliVity Gen11 Firmware v2025_1001 or later

RECOMMENDATIONS:

- Apply Firmware Updates Immediately-Upgrade HPE SimpliVity Gen11 Firmware to fixed version or later.

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.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04935en_us&docLocale=en_US