مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Remote Code Execution Vulnerability in HPE OneView Software

Tracking #:432318141

Date:17-12-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Hewlett Packard Enterprise (HPE) has released a security bulletin addressing a critical remote code execution (RCE) vulnerability affecting HPE OneView Software.

TECHNICAL DETAILS:

Hewlett Packard Enterprise (HPE) has released a security bulletin addressing a critical remote code execution (RCE) vulnerability affecting HPE OneView Software. Identified as CVE-2025-37164, this flaw allows a remote, unauthenticated attacker to execute arbitrary code on affected systems. The vulnerability has been assigned a CVSS v3.1 base score of 10.0 (Critical), indicating maximum severity and potential for full system compromise. Immediate remediation is strongly recommended.

Vulnerability Details

- **CVE ID:** CVE-2025-37164
- **CVSS Base Score:** 10.0 (Critical)
- **Vulnerability Type:** Remote Code Execution
- **Attack Vector:** Network
- **Authentication Required:** None
- **User Interaction:** None
- **Affected Products**
  - HPE OneView – All versions prior to v11.00
- **Fixed Version**
  - HPE OneView v11.00 or later

RECOMMENDATIONS:

- Immediate Action (Critical Priority):Upgrade all affected HPE OneView deployments to fixed version or later without delay.
- Apply Security Hotfixes Where Upgrade Is Not Immediately Possible
  - Deploy the HPE-provided security hotfix for versions 5.20–10.20.
  - Ensure hotfix reapplication after any appliance upgrade or reimage.

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=hpesbgn04985en_us&docLocale=en_US