مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in HPE StoreOnce Software

Tracking #:432317340

Date:03-06-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Hewlett Packard Enterprise (HPE) has disclosed multiple critical vulnerabilities in HPE StoreOnce Software.

TECHNICAL DETAILS:

Hewlett Packard Enterprise (HPE) has disclosed multiple critical vulnerabilities in HPE StoreOnce Software, which are tracked under CVE-2025-37089 through CVE-2025-37096. These vulnerabilities—some of which require no authentication—could allow remote code execution, server-side request forgery (SSRF), authentication bypass, arbitrary file deletion, and information disclosure through directory traversal attacks.

Vulnerability Details:

CVE ID	Title / Type	CVSS v3.1 Base Score
CVE-2025-37093	Authentication Bypass	9.8 (Critical)
CVE-2025-37089	Remote Code Execution	7.2 (High)
CVE-2025-37090	Server-Side Request Forgery (SSRF)	5.3 (Medium)
CVE-2025-37091	Remote Code Execution	7.2 (High)
CVE-2025-37092	Remote Code Execution	7.2 (High)
CVE-2025-37094	Directory Traversal / Arbitrary File Deletion	5.5 (Medium)
CVE-2025-37095	Directory Traversal / Information Disclosure	4.9 (Medium)
CVE-2025-37096	Remote Code Execution	7.2 (High)

Affected Products:

- HPE StoreOnce VSA versions prior to 4.3.11.

Fixed Versions:

- HPE StoreOnce Software version 4.3.11 or later

RECOMMENDATIONS:

- Upgrade HPE StoreOnce Software version to fixed version or later as soon as possible.

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=hpesbst04847en_us&docLocale=en_US