مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Privilege Escalation Vulnerability in NetApp SnapCenter

Tracking #:432317013

Date:26-03-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical privilege escalation vulnerability (CVE-2025-26512, CVSS 9.9) has been identified in NetApp SnapCenter, a centralized data protection platform for hybrid cloud environments.

TECHNICAL DETAILS:

A critical privilege escalation vulnerability (CVE-2025-26512, CVSS 9.9) has been identified in NetApp SnapCenter, a centralized data protection platform for hybrid cloud environments. The flaw allows authenticated SnapCenter users to gain administrative privileges on remote systems where SnapCenter plug-ins are installed. NetApp has released patches for affected versions, and immediate remediation is required to prevent unauthorized access to sensitive data and critical infrastructure.

Vulnerability Details

- **CVE Identifier**: CVE-2025-26512
- **CVSS Score**: 9.9 (Critical)
- **Affected Software**:
  - SnapCenter versions prior to **6.0.1P1** and **6.1P1**
- **Impact**:
  - Privilege Escalation: Enables an authenticated user to gain administrative privileges on remote systems running SnapCenter plug-ins.
  - Unauthorized Access: Potential access to sensitive data and system control.
  - System Compromise: Attackers could execute administrative actions, modify critical configurations, or deploy malicious payloads.

RECOMMENDATIONS:

- Upgrade SnapCenter to the fixed versions immediately via the NetApp Support Portal.
- Review system logs for unexpected user privilege changes or unauthorized access attempts.

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://security.netapp.com/advisory/ntap-20250324-0001/