مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Multiple Vulnerabilities in IBM Security Verify Directory

Tracking #:432316848

Date:10-02-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in IBM Security Verify Directory that could potentially be exploited to gain control over critical system functions.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2024-51450 (CVSS 9.1 Critical):** Remote Command Injection.
  - This critical vulnerability allows a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. This could lead to complete system compromise.
  - CVE-2024-51450 poses a severe risk as it could enable attackers to remotely execute commands on affected systems, leading to potential data breaches, system compromise, and unauthorized access.
- **CVE-2024-49814 (CVSS 7.8 High):** Local Privilege Escalation.
  - This high-severity vulnerability allows an authenticated local user to gain elevated privileges, potentially leading to system takeover.
  - Exploitation of CVE-2024-49814 could allow attackers to escalate privileges and gain control over critical system functions.

Affected Versions:

- IBM Security Verify Directory Server Container versions 10.0.0 through 10.0.3

Fixed Version:

- IBM Security Verify Directory, Version 10.0.3.1

RECOMMENDATIONS:

- Apply the security patch available on IBM's official support page for IBM Security Verify Directory.
- **Review System Logs**: Monitor logs for any unusual activity that may indicate potential exploitation attempts.
- **Restrict Access**: Limit access to administrative functions and ensure strong authentication mechanisms are in place.
- **Follow IBM Security Guidelines**: Adhere to IBM's recommended security best practices to minimize risk

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://www.ibm.com/support/pages/node/7182558