



مجلس الأمن السيبراني

CYBER SECURITY COUNCIL



United Arab Emirates

Exploited Vulnerability in Acronis Cyber Infrastructure

Tracking #:432316102

Date:30-07-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical vulnerability in Acronis Cyber Infrastructure is currently being exploited in the wild.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2023-45249** | CVSS score: **9.8 - Critical** | Insecure Default Password Vulnerability
 - The security defect impacts Acronis Cyber Infrastructure (ACI) and allows threat actors to execute arbitrary code remotely due to the use of default passwords.

Affected Versions:

- Acronis Cyber Infrastructure (ACI) before build 5.0.1-61
- Acronis Cyber Infrastructure (ACI) before build 5.1.1-71
- Acronis Cyber Infrastructure (ACI) before build 5.2.1-69
- Acronis Cyber Infrastructure (ACI) before build 5.3.1-53
- Acronis Cyber Infrastructure (ACI) before build 5.4.4-132

Fixed Versions:

- Acronis Cyber Infrastructure 5.4 update 4.2
- Acronis Cyber Infrastructure 5.2 update 1.3
- Acronis Cyber Infrastructure 5.3 update 1.3
- Acronis Cyber Infrastructure 5.0 update 1.4
- Acronis Cyber Infrastructure 5.1 update 1.2

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Acronis.

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-advisory.acronis.com/advisories/SEC-6452>