مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in NAKIVO Backup & Replication

Tracking #:432316916

Date: 28-02-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been identified in NAKIVO Backup & Replication that allows an unauthenticated attacker to read arbitrary files on the host system, including sensitive configuration files, logs, and database files.

TECHNICAL DETAILS:

A critical unauthenticated Arbitrary File Read vulnerability has been discovered in NAKIVO Backup & Replication version 10.11.3.86570 and potentially earlier versions. This vulnerability, tracked as **CVE-2024-48248**, allows an unauthenticated attacker to read arbitrary files on the host system, including sensitive configuration files, logs, and database files.

Exploitation of this vulnerability could lead to the exposure of credentials, backup data, and other critical information, potentially enabling attackers to compromise integrated systems such as cloud environments, hypervisors, and domain controllers.

NAKIVO has silently patched the vulnerability in version **11.0.0.88174**, but no public advisory or CVE assignment was issued by the vendor.

Key Details:

- **CVE ID**: CVE-2024-48248
- **Vulnerability Type**: Unauthenticated Arbitrary File Read
- **Affected Product**: NAKIVO Backup & Replication (version 10.11.3.86570 and potentially earlier)
- **Fixed Version**: 11.0.0.88174
- **Impact**: High,
  - Attackers can read sensitive files, including:
  - Configuration files (config.properties)
  - Database files (product01.h2.db)
  - Log files (backup.log, controller-physical.log)
  - Backup files (.raw)
  - By extracting credentials from the database or configuration files, attackers can gain access to integrated systems such as AWS S3 buckets, SSH servers, and domain controllers.
- **PoC**: A proof-of-concept (PoC) tool for detecting the vulnerability is available on GitHub

RECOMMENDATIONS:

- Update NAKIVO Backup & Replication to Fixed version at the earliest.
- Restrict access to the NAKIVO Backup & Replication Director Web Interface to trusted IP addresses only.

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://labs.watchtowr.com/the-best-security-is-when-we-all-agree-to-keep-everything-secret-except-the-secrets-nakivo-backup-replication-cve-2024-48248/