مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Nimesa Backup and Recovery
Tracking #:432317461
Date:08-07-2025

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities have been identified in Nimesa Backup and Recovery, a widely used data protection and disaster recovery solution.

TECHNICAL DETAILS:

Multiple vulnerabilities have been identified in Nimesa Backup and Recovery, a widely used data protection and disaster recovery solution. These include an **OS command injection** vulnerability (CVE-2025-48501) and a **Server-Side Request Forgery (SSRF)** vulnerability (CVE-2025-53473). Successful exploitation could allow unauthenticated attackers to execute arbitrary commands on the host system or make unauthorized internal network requests.

Vulnerability Details

1. **CVE-2025-48501 – OS Command Injection**
   - **Type**: Command Injection (CWE-78)
   - **Affected Versions**:
     - v2.3
     - v2.4
   - **CVSS v4.0 Score**: 9.3 (Critical)
   - **CVSS v3.0 Score**: 9.8 (Critical)

2. **CVE-2025-53473 – Server-Side Request Forgery (SSRF)**
   - **Type**: SSRF (CWE-918)
   - **Affected Versions**:
     - v2.3
     - v2.4
     - All versions prior to v3.0.2025062305
   - **CVSS v4.0 Score**: 6.9 (High)
   - **CVSS v3.0 Score**: 7.3 (High)

RECOMMENDATIONS:

- Immediately upgrade Nimesa Backup and Recovery to fixed version.

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://nvd.nist.gov/vuln/detail/CVE-2025-48501
- https://nvd.nist.gov/vuln/detail/CVE-2025-53473

https://www.csc.gov.ae

TLP: WHITE