مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Critical Vulnerabilities in Nginx UI

Tracking #:432318693

Date:31-03-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Nginx UI that could allow unauthenticated attackers to gain full control over affected systems or achieve persistent compromise through tampered backups.

TECHNICAL DETAILS:

Multiple critical vulnerabilities have been identified in **Nginx UI**, a web-based management interface for Nginx. These flaws could allow unauthenticated attackers to gain full control over affected systems or achieve persistent compromise via tampered backups. Public proof-of-concept (PoC) exploit code is available for both issues, increasing the risk of active exploitation.

Vulnerability Details

1. Authentication Bypass via MCP Endpoint

- **CVE ID:** CVE-2026-33032
- **Severity:** Critical **CVSS Score:** 9.8
- This vulnerability exists in the Model Context Protocol (MCP) integration of Nginx UI. The /mcp_message endpoint is not protected by authentication and instead relies on an IP whitelist. Due to a design flaw, an empty whitelist is treated as "allow all," enabling any remote attacker to access the endpoint without authentication.
- This allows attackers to invoke MCP tools and fully control Nginx configurations and services.

Impact

- Unauthorized access to administrative functionality
- Traffic interception and redirection
- Exposure of sensitive configurations
- Credential harvesting
- Service disruption or complete takeover

2. Backup/Restore Mechanism Integrity Bypass

- **CVE ID:** CVE-2026-33026
- **Severity:** Critical **CVSS Score:** 9.4
- This vulnerability is caused by a flawed cryptographic design in the backup and restore mechanism. Backup archives are encrypted using AES-256-CBC, but the encryption key and IV are exposed to the client. Integrity metadata is also encrypted using the same key, allowing attackers to modify backups, recompute hashes, and repackage them as valid.
- Additionally, the restore process does not strictly enforce integrity checks and may accept tampered backups even when verification fails.

Impact

- Backup tampering and malicious configuration injection
- Persistent backdoor insertion
- Arbitrary command execution
- Full system compromise

Affected Products

- **CVE-2026-33032:** All versions of Nginx UI
- **CVE-2026-33026:** Nginx UI versions up to and including **2.3.3**

Fixed Versions

CVE-2026-33032

- Currently No official patch available

CVE-2026-33026

- Nginx UI **2.3.4** or later

RECOMMENDATIONS:

- Apply the mitigations or workarounds recommended by Nginx UI
- Apply security updates and patches as soon as they become available
- Limit exposure of management interfaces to trusted environments
- Implement strong authentication and access controls
- Regularly monitor systems and logs for suspicious activity
- Follow secure configuration and hardening best practices
- Maintain regular backups and verify their integrity before use

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-2026-33032
- https://nvd.nist.gov/vuln/detail/CVE-2026-33026