INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-18 17:21 UTC

CVE-2026-50268: Plaintext Password Storage in SteeltoeOSS Steeltoe.Configuration.Encryption

CVE VULNERABILITY | LOW | CVSS 3.3

SCC Item ID	SCC-CVE-2026-0332
Type	CVE Vulnerability
CVE ID	CVE-2026-50268
Severity	LOW
CVSS Base Score	3.3
Affected Products	SteeltoeOSS Steeltoe.Configuration.Encryption (version range unconfirmed, source: gemini, unverified)
Published	2026-06-17
Discovery Source	Gemini

Executive Summary

CVE-2026-50268 describes a plaintext password storage flaw (CWE-256) in SteeltoeOSS Steeltoe.Configuration.Encryption, a .NET library designed specifically to protect sensitive configuration values in cloud-native microservices environments. Any attacker who gains access to the filesystem, configuration files, or memory of an affected host can retrieve credentials in cleartext, no decryption required. The affected version range and patch status are not yet confirmed by NVD or CISA; organizations using Steeltoe in production should monitor NVD and the SteeltoeOSS GitHub releases page for confirmed affected version information and patch availability.

Technical Analysis

CVE-2026-50268 is a CWE-256 (Plaintext Storage of a Password) weakness in the SteeltoeOSS Steeltoe.Configuration.Encryption module. The module is designed to encrypt sensitive values within .NET microservice configuration pipelines; however, the reported flaw indicates credentials are stored without encryption at rest. Exploitation maps to MITRE ATT&CK T1552.001 (Credentials in Files), where an attacker with local filesystem access, the ability to read configuration files, or the ability to capture a memory dump can extract credentials directly. No CVSS vector string has been confirmed by NVD. The pipeline-assigned CVSS base score is 3.3 (Low). EPSS score is 0.0; the vulnerability does not appear on the CISA KEV catalog as of this analysis. Affected version range is unconfirmed pending NVD publication. Authoritative patch or remediation guidance from SteeltoeOSS or NVD has not been confirmed at time of writing.

Action Checklist

1. Step 1: Containment, Identify all services using Steeltoe.Configuration.Encryption in your .NET microservice deployments. Restrict filesystem and configuration-file read access to only the service accounts that require it, applying least-privilege principles per NIST AC-6. Audit cloud-native secret stores (e.g., Vault, Azure Key Vault, AWS Secrets Manager) to confirm credentials are not also stored in plaintext configuration files alongside Steeltoe config.
2. Step 2: Detection, Search application configuration files, environment variable stores, and deployment manifests for plaintext credential strings on hosts running Steeltoe-based services. Review audit logs for unexpected file reads or access to configuration directories (NIST AU-2, AU-6; CIS 8.2). Apply file integrity monitoring (FIM) to monitor configuration files for unauthorized access or modification. Query SIEM for T1552.001 behavioral patterns: unusual process access to config files, credential-shaped strings in file-read events.
3. Step 3: Eradication, Monitor the official SteeltoeOSS GitHub repository and NVD entry for CVE-2026-50268 for a confirmed patch or remediation advisory. Until a patch is available, migrate sensitive credentials out of Steeltoe.Configuration.Encryption storage and into a dedicated secrets management solution with encryption at rest enforced at the platform layer. Rotate all credentials that may have been stored in plaintext per NIST IA-4 (Credential Management).
4. Step 4: Recovery, After credential rotation and migration to a verified secrets store, validate that no plaintext credentials remain in configuration files, environment variable exports, or container image layers. Re-enable services under monitoring with enhanced file-integrity alerting on configuration paths. Verify NIST AU-9 (Protection of Audit Information) controls are in place to protect the audit trail from tampering during the recovery window.
5. Step 5: Post-Incident, Document the control gap: a component explicitly named 'Encryption' failed to encrypt. Review your software inventory (CIS 2.1) and procurement criteria to require verification of encryption-at-rest behavior for all credential-handling libraries before adoption. Establish a recurring check against NVD and the SteeltoeOSS advisory channel for this CVE as patch details emerge. Map the gap to NIST IA controls for credential management and schedule a follow-up review. Monitor NVD and the SteeltoeOSS GitHub releases page for patch availability, as of publication, no official patch has been released.

Detection Guidance

Search all .NET microservice hosts and container images for configuration files (appsettings.json, appsettings.*.json, environment variable files) containing credential-shaped values (passwords, connection strings, API keys) that are stored without an encryption wrapper. Use file integrity monitoring (FIM) / system file analysis to flag unauthorized reads of configuration paths. In your SIEM, build a detection for MITRE T1552.001: processes accessing configuration files outside normal service account context, especially at elevated frequency or from unexpected parent processes. Enable NIST AU-2 event logging for file-read operations on configuration directories. CIS 8.2 requires audit log collection across enterprise assets; confirm this is active on all hosts running Steeltoe-based services. No confirmed IOC patterns (hashes, IPs, domains) are available for this CVE; detection is behavioral and configuration-state-based.

Framework Mappings

MITRE-ATTACK

- **T1552.001** — Credentials In Files

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.312(e)(1)** — Transmission Security

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.8.24** — Use of cryptography
- **A.5.23** — Information security for use of cloud services

NIST-800-53R5

- **SC-13** — Cryptographic Protection

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1552.001	Credentials In Files	Credential-Access

Sources

Source	URL	Tier
Security Bulletin: February 6, 2026 - n8n Community	https://community.n8n.io/t/security-bulletin-february-6-2026/261682...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-50268	T1

Generated 2026-06-18 17:21 UTC by TJS Security Command Center