NCA-10.140326 – National CERT Advisory

Critical Remote Code Execution Vulnerabilities in n8n Workflow Automation Platform (Multiple CVEs)

Multiple critical vulnerabilities have been identified in the **n8n Workflow Automation Platform** that could allow attackers to execute arbitrary commands on the host system and expose sensitive credentials stored within the platform. The most severe issues include **CVE-2026-27577** and **CVE-2026-27493**, with CVSS scores of **9.4** and **9.5** respectively.

The vulnerabilities arise from improper sandbox isolation within the expression compiler and double expression evaluation in publicly accessible form endpoints. When exploited together, these flaws may allow attackers to escalate from **unauthenticated input to full remote code execution (RCE)** on the n8n server. Successful compromise could expose sensitive environment variables such as **N8N_ENCRYPTION_KEY**, enabling attackers to decrypt stored credentials and gain persistent access to integrated services and infrastructure.

Two additional critical vulnerabilities, **CVE-2026-27495** and **CVE-2026-27497**, have also been addressed by the vendor. Immediate remediation is strongly recommended for all affected deployments.

DOCUMENT SUMMARY

Advisory ID	NCA-10.140326
Threat Type	Remote Code Execution / Expression Injection / Credential Exposure
Severity	Critical
Attack Vector	Network (Remote)
Authentication Required	No (in certain exploitation scenarios)
User Interaction	None
CVSS Score	Up to 9.5 (Critical – Remote System Compromise)
CVE IDs	CVE-2026-27577, CVE-2026-27493, CVE-2026-27495, CVE-2026-27497
Affected Product	n8n Workflow Automation Platform

IMPACT ANALYSIS

Successful exploitation may result in:

1. **Remote Code Execution (RCE)** – Execution of arbitrary system commands on the n8n host
2. **Credential Exposure** – Access to stored credentials encrypted within the platform
3. **Environment Variable Leakage** – Exposure of sensitive variables including encryption keys
4. **Workflow Manipulation** – Injection of malicious workflow logic
5. **Privilege Escalation** – Escalation from limited user access to system-level command execution
6. **Service Integration Compromise** – Unauthorized access to connected APIs, cloud services, and databases
7. **Lateral Movement** – Pivoting from compromised automation servers into internal infrastructure
8. **Data Exfiltration** – Unauthorized access to workflow data and integrated service responses
9. **Persistence Mechanisms** – Creation of malicious workflows or triggers for long-term access
10. **Operational Disruption** – Manipulation or disabling of business automation processes

THREAT CHARACTERISTICS

Characteristic	Details
Threat Category	Remote Code Execution / Expression Injection
Threat Status	Publicly Disclosed

Root Cause	Sandbox escape and double expression evaluation in workflow expressions
Attack Complexity	Low to Moderate
Privileges Required	None or Low (depending on attack path)
User Interaction	None
Exposure Risk	Highest where form endpoints or workflow editing capabilities are publicly accessible
Affected Deployments	Self-hosted and cloud deployments of n8n
CWE Classifications	CWE-94 (Code Injection), CWE-284 (Improper Access Control), CWE-94 (Improper Control of Code Generation), CWE-522 (Insufficiently Protected Credentials)

AFFECTED SYSTEMS

The following versions of **n8n Workflow Automation Platform** are affected:

- Versions **prior to 1.123.22**
- Version **2.0.0 through 2.9.2**
- Version **2.10.0**

Patched releases:

- **1.123.22**
- **2.9.3**
- **2.10.1**

Systems are particularly at risk when:

- Public **Form endpoints** are enabled
- Workflow creation permissions are granted broadly
- Instances are **internet-exposed**
- Credentials are stored within workflows or nodes

INDICATORS OF COMPROMISE (IoCs)

1. Unexpected execution of system commands originating from the n8n service
2. Unknown or suspicious workflow expressions or nodes appearing in workflows
3. Unauthorized modifications to existing workflows
4. Suspicious activity targeting public form endpoints
5. Exposure or access attempts to environment variables (e.g., `N8N_ENCRYPTION_KEY`)
6. Unusual outbound network connections from the n8n server
7. Unexpected credential usage against integrated APIs or services
8. New workflows or triggers created without administrative approval
9. Abnormal log entries related to expression evaluation or script execution
10. Indicators of privilege escalation within the n8n application

REMEDIATION ACTIONS

Action Category	Specific Actions	Priority
Immediate Patching	Upgrade to n8n versions 2.10.1, 2.9.3, or 1.123.22	**MANDATORY**
Access Control	Restrict workflow creation/editing privileges to trusted administrators	**HIGH**
Workflow Review	Audit existing workflows for malicious expressions or scripts	**REQUIRED**
Credential Hygiene	Rotate credentials stored in the n8n environment	**REQUIRED**
Platform Hardening	Deploy n8n in a hardened environment with restricted OS privileges	**HIGH**

Network Security	Limit external exposure and restrict access to management interfaces	**HIGH**

Temporary Mitigation (if immediate patching is not feasible):

Disable vulnerable nodes via environment variables:

- Disable Form node:
  `NODES_EXCLUDE=n8n-nodes-base.form`
- Disable Form Trigger node:
  `NODES_EXCLUDE=n8n-nodes-base.formTrigger`
- Disable Merge node:
  `NODES_EXCLUDE=n8n-nodes-base.merge`

Run JavaScript tasks in external runner mode:

```
N8N_RUNNERS_MODE=external
```

Note: Mitigation measures only reduce risk and **do not eliminate the vulnerability**. Patching remains the only complete remediation.

ACTION SUMMARY & RESPONSE PRIORITIES

Action Type	Specific Steps	Priority	Timeframe
Patch Deployment	Upgrade to patched n8n releases	**MANDATORY**	**Immediate**
Exposure Reduction	Restrict public access to form endpoints and workflow interfaces	**HIGH**	**Immediate**
Workflow Audit	Review all workflows for suspicious expressions	**HIGH**	**Within 24–48 hours**
Credential Rotation	Reset stored credentials and API keys	**HIGH**	**Within 72 hours**
Log Review	Conduct compromise assessment of automation server	**REQUIRED**	**Immediate**
Continuous Monitoring	Implement monitoring for abnormal expression execution	**REQUIRED**	**Ongoing**

MONITORING & DETECTION REQUIREMENTS

#	Monitoring Activity
1	Monitor logs for suspicious expression evaluation or command execution
2	Detect creation or modification of workflows without authorization
3	Alert on access attempts to environment variables
4	Monitor public form endpoints for injection attempts
5	Detect abnormal outbound connections from automation servers
6	Integrate n8n logs with SIEM for anomaly detection
7	Monitor credential usage for integrated services
8	Review changes to node configurations and workflow triggers

REFERENCES

Reference	URL
NVD Vulnerability Database	https://nvd.nist.gov/vuln/search/#/nvd/home?keyword=CVE-2026-27577
GitHub Security Advisories	https://github.com/n8n.io/n8n/security/advisories
Official n8n Security Page	https://n8n.io/legal/security/
Ciser Safety	https://cisersafety.com/en/cve-2026-27577-n8n-critical-vulnerabilities-rce/

ArmeSec Analysis	https://www.armesec.io/blog/four-critical-rce-vulnerabilities-in-n8n-what-cloud-security-teams-need-to-know/
SentinelOne Vulnerability Database	https://www.sentinelone.com/vulnerability-database/cve-2026-27493/

CALL TO ACTION – KEY IMPERATIVES

#	Requirement
1	Treat these vulnerabilities as mission-critical
2	Immediately patch all affected n8n instances
3	Restrict workflow editing capabilities to trusted users
4	Disable vulnerable nodes if patching is temporarily delayed
5	Rotate all stored credentials and encryption keys
6	Conduct a full compromise assessment if the instance was publicly exposed
7	Implement monitoring for malicious workflow activity

WARNING: Failure to remediate these vulnerabilities may result in **complete server compromise, credential exposure, data exfiltration, and persistent attacker access to integrated enterprise services and infrastructure. Immediate action is required.**