مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Unauthenticated Remote Code Execution Vulnerabilities in n8n

Tracking #:432318573

Date:12-03-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Security researchers have identified two critical vulnerabilities affecting the workflow automation platform n8n.

TECHNICAL DETAILS:

Security researchers have identified two critical vulnerabilities affecting the workflow automation platform n8n. The vulnerabilities allow attackers to execute arbitrary commands on affected servers and potentially compromise sensitive credentials stored within the platform.

Vulnerability Breakdown
1. CVE-2026-27493 — Unauthenticated Zero-Click Remote Code Execution
Description:
A critical vulnerability in n8n Form nodes allows attackers to exploit a double-evaluation flaw in the expression engine. When a multi-step form renders user input back to the submitter using an HTML rendering step, the input may be interpreted as an expression and evaluated twice. This behavior allows attackers to inject expressions that execute arbitrary shell commands on the server.

Key Details

- **CVE ID: CVE-2026-27493**
- Severity: Critical
- CVSS v4.0 Score: 9.5
- Vector: CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H
- Authentication Required: No

Technical Characteristics

- Zero-click exploitation
- No authentication required
- Triggered through public multi-step form endpoints
- Exploits expression injection during form rendering

2. CVE-2026-27577 — Sandbox Escape in Expression Compiler
Description:
A sandbox escape vulnerability exists in the expression compiler used by n8n. Due to a missing case in the AST (Abstract Syntax Tree) rewriter, certain expression structures such as SpreadElement are not properly transformed. This allows attackers to bypass sandbox protections and gain access to the underlying Node.js environment.
Key Details

- CVE ID: **CVE-2026-27577**
- Severity: Critical
- CVSS v4.0 Score: 9.4
- Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H
- Authentication Required: Yes

Technical Characteristics

- Sandbox escape in the expression evaluation engine
- Triggered through crafted expressions
- Allows direct interaction with system processes

Patched Versions

- n8n 2.10.1
- n8n 2.9.3
- n8n 1.123.22

RECOMMENDATIONS:

- Organizations using n8n should upgrade to a patched version immediately.

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-2026-27493
- https://nvd.nist.gov/vuln/detail/CVE-2026-27577