مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical RCE Vulnerability in protobuf.js

Tracking #:432318802

Date:17-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical Remote Code Execution (RCE) vulnerability (CVSS 9.4) has been identified in protobuf.js, a widely used JavaScript implementation of Protocol Buffers.

TECHNICAL DETAILS:

A critical Remote Code Execution (RCE) vulnerability (CVSS 9.4) has been identified in protobuf.js, a widely used JavaScript implementation of Google Protocol Buffers with massive adoption across Node.js and browser ecosystems.
The flaw allows attackers to inject and execute arbitrary JavaScript code during the decoding of malicious protobuf definitions. While exploitation requires control over .proto or JSON descriptor inputs, environments that support dynamic or external schema loading are at significant risk of full system compromise.
Immediate remediation is required due to the library's extensive usage and the severity of impact.

Vulnerability Details:

- Type: Remote Code Execution (RCE)
- Severity: Critical (CVSS 9.4)
- Component Affected: Parsing and compilation of protobuf definitions
- Attack Vector: Malicious .proto or JSON descriptor files
- Proof of concept: Available

Exploitation Mechanism

- Attackers craft a malicious protobuf schema (JSON or .proto).
- Inject arbitrary JavaScript payloads into type definitions.
- When the application invokes:
- Type.decode() or similar decoding functions
- The injected payload is executed within the application runtime.

Affected Versions

- 8.x: ≤ 8.0.0
- 7.x: ≤ 7.5.4

Patched Versions

- 8.0.1
- 7.5.5

RECOMMENDATIONS:

- **Patch Immediately**:
  - Upgrade urgently to patched versions.

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://github.com/protobufjs/protobuf.js/security/advisories/GHSA-xq3m-2v4x-88gg