Severity

High

Analysis Summary

CVE-2022-21803

Node.js nconf module could allow a remote attacker to execute arbitrary code on the system, caused by a prototype pollution flaw when using the memory engine. By adding or modifying properties of Object.prototype using a proto or constructor payload, an attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.

Impact

Code Execution

Indicators Of Compromise

CVE

CVE-2022-21803

Affected Vendors

Node.js

Affected Products

Node.js nconf 0.11.3

Remediation

Upgrade to the latest version of nconf, available from the nconf GIT Repository.

nconf GIT Repository