SVR.JS

SECURITY ADVISORY FOR SVR.JS

Advisory ID: SVRJS-00002

Date: September 6, 2023

Affected software

- **SVR.JS**, from 3.3.1 to 3.9.1 and 3.4.29

Categories

- **CWE-22** – Improper Limitation of a Pathname to a Restricted Directory

Vulnerability description

SVR.JS 3.3.1 has moved from depreciated *url.parse* function to custom wrapper over WHATWG URL parser. The WHATWG URL parser sanitizes some path traversal strings, like "*../../../../../../../../../../etc/passwd*". Those versions of SVR.JS didn't change *req.url* property to reflect URL sanitized by WHATWG URL parser. As a result, SVR.JS mods and server-side JavaScript using *req.url* property on affected SVR.JS versions may be vulnerable to path traversal (not including queries).

Mitigation

Users should either upgrade SVR.JS to newer version, or remove unneeded SVR.JS mods. SVR.JS instances without any mods nor server-side JavaScript are not affected.

Patch details

Newer versions of SVR.JS change *req.url*, if it detects, that WHATWG parser sanitized URLs by comparing original *req.url* with concatenation of *pathname*, *search* and *hash* properties of *URL* object.

Update instructions

Read SVR.JS documentation in order to upgrade SVR.JS to new unaffected versions

Additional recommendations

Users should generally update their server software to be safe from security vulnerabilities.