SVR.JS

SECURITY ADVISORY FOR SVR.JS

Advisory ID: SVRJS-00003

Date: September 7, 2023

Affected software

- **SVR.JS**, older than 3.9.3 and 3.4.31

Categories

- **CWE-284** – Improper Acces Control

Vulnerability description

Affected versions executed both non-proxy SVR.JS mods and server-side JavaScript non-proxy callbacks, even if the request URL began with "*http://*" or with "*https://*" instead of "*/*". SVR.JS doesn't enforce URL rewriting nor non-standard codes (for 403 Forbidden status code and HTTP authentication) on proxy requests to avoid interference of it's access controls with proxy SVR.JS mods. As a result, attacker could use those request URLs to bypass access controls of those affected SVR.JS versions.

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

Patched versions of SVR.JS don't execute function returned by *callback* method of *Mod* object, if the request URL begins with "*http://*" or with "*https://*", unless *proxyCallback* method of *Mod* object is present. Many SVR.JS mods that are not proxies don't have *proxyCallback* method present in *Mod* object. As a result, patched versions don't execute non-proxy SVR.JS mods nor server-side JavaScript to avoid access control bypass vulnerabilities.

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. Mods utilizing *proxyCallback* method also should have proxy URL check to avoid access control bypass vulnerabilities.