SVR.JS

SECURITY ADVISORY FOR SVR.JS

Advisory ID: SVRJS-00004

Date: September 10, 2023

Affected software

- **SVR.JS**, older than 3.9.6 and 3.4.34

Categories

- **CWE-200** – Exposure of Sensitive Information to an Unauthorized Actor
- **CWE-552** – Files or Directories Accessible to External Parties

Vulnerability description

Affected versions don’t have *temp* directory inside SVR.JS installation in forbidden path list. Affected versions only added *modloader* directory and *serverSideScript.js* file in *temp* directory (not *.modloader_w12345* nor *.serverSideScript_w12345.js*) when *disableServerSideScriptExpose* property in *config.json* file is set to *true*. As a result, attacker could use URL beginning with "*/temp/*" to leak information from temp directory in SVR.JS installation directory (includes source code through hidden *.modloader_w12345* and *.serverSideScript_w12345.js*), if web root is in SVR.JS installation directory.

Mitigation

Users should either upgrade SVR.JS to newer patched versions, or set up 403 code for URLs beginning with */temp/* in non-standard codes. SVR.JS instances with web roots outside SVR.JS installation directories are not affected.

Patch details

Patched SVR.JS versions have entire *temp* directory inside SVR.JS installation directory in the list of forbidden paths.

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.