SVR.JS

SECURITY ADVISORY FOR SVR.JS

Advisory ID: SVRJS-00005

Date: February 2, 2023

Affected software

- **RedBrick**, older than 2.5.4
- **OrangeCircle**, older than 1.1.2
- **YellowSquare**, older than 1.1.2

Categories

- **CWE-287** – Improper Authentication

Vulnerability description

The affected SVR.JS mod versions didn’t check, if the HTTP authentication was required or not. Some web applications (like *git-http-backend*) enable some functionality based on the *REMOTE_USER* environment value (or *remoteUser* JSGI property). The affected mods set *REMOTE_USER* variable based only on the presence of the *Authorization* HTTP header and not on the HTTP authentication requirement (401 non-standard code in the *config.json* file).

As a result, an attacker could add the *Authorization* header, when the authorization is not required. Affected mods would then set the *REMOTE_USER* environment variable (or *remoteUser* JSGI property), that will cause some web applications to think that the client is authenticated. Consequently, the functionality will be enabled because of “broken” authentication.

Mitigation

Users should either upgrade affected mods to newer patched versions or disable unneeded web application functionality (that is enabled by default, when authenticated) via web application configuration.

Patch details

Newer versions of RedBrick, OrangeCircle and YellowSquare are first trying using the *authUser* property set by SVR.JS 3.14.2 and newer versions, and when the property is missing (in case of older SVR.JS versions), then it will fall back to checking the configuration file for matching 401 non-standard code definitions. If there are no matching definitions, then authentication-related properties will not be set.

Update instructions

To update those mods to newer patched versions (RedBrick 2.5.4, OrangeCircle 1.1.2, YellowSquare 1.1.2), delete old mods inside *mods* directory in the SVR.JS installation directory, then copy new mod archives to mods directory. Restart SVR.JS for changes to take effect.

Additional recommendations

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