SVR.JS

SECURITY ADVISORY FOR SVR.JS

Advisory ID: SVRJS-00001

Date: August 14, 2023

Affected software

- **RedBrick**, older than 2.3.3
- **reverse-proxy-mod**, older than 1.0.4
- **OrangeCircle**, older than 1.0.2
- **YellowSquare**, older than 1.0.1

Categories

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

Vulnerability description

In RedBrick versions older than 2.3.3, attacker could use "*CGI-BIN*" instead of "*cgi-bin*" to leak CGI application source code, when SVR.JS with RedBrick is run on Windows. This is because Windows paths are case-sensitive, and RedBrick checking function present in these versions is always case-insensitive. The same applies to "*redbrick-interpreters.json*" file leaking RedBrick interpreter configuration.

In OrangeCircle versions older than 1.0.2, attacker could leak OrangeCircle configuration from "*orangecircle-config.json*" file for the same reasons mentioned above.

In YellowSquare versions older than 1.0.1, attacker could use "*JSGI-BIN*" instead of "*jsgi-bin*" to leak JSGI application source code, when SVR.JS with YellowSquare is run on Windows, for the same reasons as RedBrick was leaking CGI application source code.

In reverse-proxy-mod versions older than 1.0.4, attacker could leak reverse proxy configuration from "*reverse-proxy-config.json*" file, because these reverse-proxy-mod versions didn't forbid this file from being accessed at all.

Mitigation

Users should either upgrade those mods to newer patched versions, set web root to directory outside SVR.JS installation directory, or disable those mods if they aren't used. Users of RedBrick, YellowSquare and OrangeCircle in SVR.JS running on non-Windows platforms are not affected.

Patch details

Newer versions of RedBrick, OrangeCircle, YellowSquare and reverse-proxy-mod have implemented case-sensitive checks, which are performed when SVR.JS is run in Windows.

Update instructions

To update those mods to newer patched versions (RedBrick 2.3.3, reverse-proxy-mod 1.0.4, OrangeCircle 1.0.2, YellowSquare 1.0.1), delete old mods inside *mods* 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.