Re: [scr966035] your CVE ID requests

cve-request@mitre.org <cve-request@mitre.org>
周二 2022/9/13 23:19
收件人:
抄送:cve-request@mitre.org <cve-request@mitre.org>

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

> [Suggested description]
> jsish 3.5.0 is vulnerable to Use after free. The function Jsi_ObjFree
> (src/jsiObj.c:342), accessed a null pointer, causing a segment fault.
>
> --
>
> [VulnerabilityType Other]
> Use after free
>
> --
>
> [Vendor of Product]
> jsish
>
> --
>
> [Affected Product Code Base]
> jsish - 3.5.0
>
> --
>
> [Affected Component]
> Jsi_ObjFree (src/jsiObj.c:342)
>
> --
>
> [Attack Type]
> Local
>
> --
>
> [Impact Denial of Service]
> true
>
> --
>
> [Attack Vectors]
> DoS attack may occur in this situation.
>
> --
>
> [Reference]
> https://github.com/pcmacdon/jsish/issues/90
>

> --
>
> [Discoverer]
>

Use CVE-2022-37838.

> [Suggested description]
> In the jsish 3.5.0, an integer overflow exits in the function
> jsiEvalCodeSub. The index of the parse stack buffer was down
> overflowed, which caused an out-of-bound read and crashed the program.
>
> --
>
> [Vulnerability Type]
> Buffer Overflow
>
> --
>
> [Vendor of Product]
> jsish
>
> --
>
> [Affected Product Code Base]
> jsish - 3.5.0
>
> --
>
> [Affected Component]
> The function jsiEvalCodeSub in the source file src/jsiEval.c
>
> --
>
> [Attack Type]
> Local
>
> --
>
> [Impact Denial of Service]
> true
>
> --
>
> [Attack Vectors]
> craft a JavaScript file parsed by the program
>
> --
>
> [Reference]
> https://github.com/pcmacdon/jsish/issues/94
>

> --
>
> [Discoverer]
> [redacted]

Use CVE-2022-38819.

> [Suggested description]
> jsish 3.5.0 is vulnerable to Buffer Overflow via src/jsiEval.c:1745. An
> integer overflow exits in the function jsiEvalCodeSub. The index of the
> parse stack buffer was down overflowed, which caused an out-of-bound
> read and crashed the program.
>
> --
>
> [Vulnerability Type]
> Buffer Overflow
>
> --
>
> [Vendor of Product]
> jsish
>
> --
>
> [Affected Product Code Base]
> jsish - 3.5.0
>
> --
>
> [Affected Component]
> src/jsiEval.c:1745
>
> --
>
> [Attack Type]
> Local
>
> --
>
> [Impact Denial of Service]
> true
>
> --
>
> [Attack Vectors]
> crafted a javascript file parsed by the program
>
> --
>
> [Reference]
> https://github.com/pcmacdon/jsish/issues/95
>
> --

>
> [Discoverer]
>

Use CVE-2022-38820.

> [Suggested description]
> In jsish 3.5.0, an integer overflow existed in the function
> jsiEvalCodeSub. The stack pointer was down overflowed, which caused an
> out-of-bound read and crashed the program.
>
> --
>
> [Vulnerability Type]
> Buffer Overflow
>
> --
>
> [Vendor of Product]
> jsish
>
> --
>
> [Affected Product Code Base]
> jsish - 3.5.0
>
> --
>
> [Affected Component]
> function jsiEvalCodeSub in the src/jsiEval.c on the line 1745
>
> --
>
> [Attack Type]
> Local
>
> --
>
> [Impact Denial of Service]
> true
>
> --
>
> [Attack Vectors]
> crafted a parsed JavaScript file for the program
>
> --
>
> [Reference]
> https://github.com/pcmacdon/jsish/issues/95?notification_referrer_id=NT_kwDOAmgbXrM0MjUwNjA2MjE2OjQwMzc3MTgy
>
> --
>

> [Discoverer]
> [redacted]

Duplicate of CVE-2022-38820

- --
CVE Assignment Team
M/S M300, 202 Burlington Road, Bedford, MA 01730 USA
 [A PGP key is available for encrypted communications at
   https://cve.mitre.org/cve/request_id.html]

```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1

iQIcBAEBCAAGBQJjIJ7fAAoJENiPHH3233OG0CsP/j5TZVJwNty0Md7NjsCc+hZK
kiRm11Rmqiw+/DQm20iagVm/QV81zPx13hcCrKLVBLyy37s/Fdwec9sBGU0N170F
Gv6UPgPj19o3wjFrKiUuRj8O8lfFrPOnXmWOiZX8rZBrz9UipL+WFQV1va+QHUXW
2HvWI1Hz/pix9/fBmbn4RRzSitsuKaNfNovHq+9Nz224c1QE5x8rU8NHiXIorrIp
961jdD2TNB3zPC1A0Zb4bE0FwZpDtWAIc0aiGhBGIA1pw4RHU1+4gwmVuwRp2+dK
hBVg3T7/0Z3vVDAfgtpDQKv5zgV0VMVA++7iJ/xHbjBikW5RikrxTg3dybOslqx0
CLRqQQZ8fsmgZb8gObxY5IqlcSFtZb35qjkOhnQ1iefgsVSfIN3dG4mLVGzErPTg
h6smCnkwrG6/k2IQ16ZGWb1sHxUGL3u5+23OrV+5MNnCIuo4+wyjxXGz5QAOQtYE
28PCxko+GTuY373x/2cmdSWx8BxDTWrY/imyBVSabbLHGj1Ccr3I23AEC3tbmBfB
fdT+OTCIu+qMIjceyauM/vUke7kS2o8DpmzzY17DDA8cXgrEkk90GN73oMNAHdRJ
bLzdonVU1LsjpsV1xMU6+j+ymdK8pj9iTRxFdy3NskAYraf1Sd/gkLRJxaj1AkhY
2ZCZn0muOgC9IOG1tNyE
=HTJG
-----END PGP SIGNATURE-----
```